PCT/JP2004/004338

日本国特許庁
JAPAN PATENT OFFICE

26. 3. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

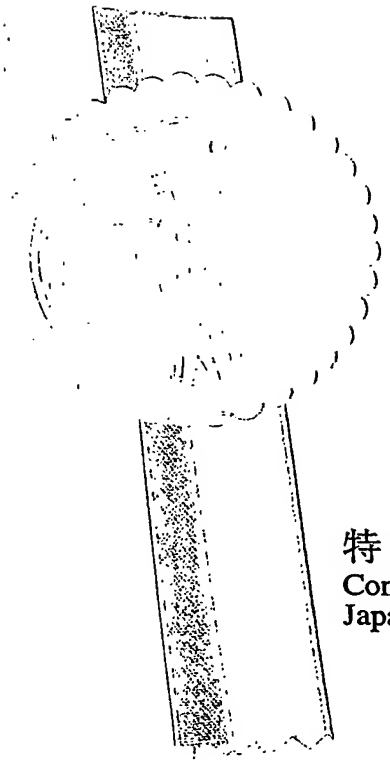
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２８日

出願番号
Application Number: 特願２００３－０９２６４７

[ST. 10/C]: [ＪＰ２００３－０９２６４７]

出願人
Applicant(s): ソニー株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年１２月　８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０１４８

【書類名】　特許願
【整理番号】　0390209013
【提出日】　平成15年 3月28日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　板橋　達夫
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラム

【特許請求の範囲】

【請求項１】　ユーザにより操作される端末と、

リソースを提供する第１の親機と、

前記ユーザの個人情報を記憶する第２の親機と、

電子バリューを管理するバリュー装置と

を備える情報処理システムにおいて、

前記端末は、

前記第１の親機が提供するリソースを要求する信号を、前記第２の親機に送信するリソース要求信号送信手段と、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する第１の利用権取得手段と

を有し、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用し、

前記第１の親機は、

前記リソースの提供に対する対価としての電子バリューが、前記第２の親機から前記第１の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記第２の親機に対して、前記利用権を発行する利用権発行手段と

を有し、

前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し、

前記第２の親機は、

前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第１の親機への前記電子バリューの振込みを、前記バリュー装置に要求する

電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記第１の親機が発行する前記利用権を取得する第２の利用権取得手段と、

前記第２の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を有し、

前記バリュー装置は、

前記第２の親機からの要求に応じて、前記第１の親機に前記電子バリューを振り込む電子バリュー振込み手段と、

前記第１の親機への前記電子バリューの振込み通知を、前記第１の親機に送信する振込み通知送信手段と

を有する

ことを特徴とする情報処理システム。

【請求項２】　ユーザにより操作される情報処理装置において、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信手段と、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得手段と

を備え、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とする情報処理装置。

【請求項３】　前記第２の親機との間で、前記ユーザが前記第２の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求項２に記載の情報処理装置。

【請求項４】　前記リソース要求信号送信手段と前記利用権取得手段は、前記第１の親機を介して、前記第２の親機とやりとりする

ことを特徴とする請求項２に記載の情報処理装置。

【請求項５】　前記リソース要求信号送信手段と前記利用権取得手段は、前記第２の親機との間で、データを暗号化してやりとりする

ことを特徴とする請求項２に記載の情報処理装置。

【請求項６】　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項２に記載の情報処理装置。

【請求項７】　ユーザにより操作される情報処理装置の情報処理方法において、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とする情報処理方法。

【請求項８】　ユーザにより操作される情報処理装置に実行させるプログラムであって、

リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、

前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する

ことを特徴とするプログラム。

【請求項９】　ユーザにより操作される端末に、自身が有するリソースを提

供する情報処理装置において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段と

を備え、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理装置。

【請求項１０】　前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項９に記載の情報処理装置。

【請求項１１】　前記振込み通知が正当であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項９に記載の情報処理装置。

【請求項１２】　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項９に記載の情報処理装置。

【請求項１３】　ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置の情報処理方法において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理方法。

【請求項１４】　ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置に実行させるプログラムであって、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とするプログラム。

【請求項１５】　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、

前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を備えることを特徴とする情報処理装置。

【請求項１６】　前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項１５に記載の情報処理装置。

【請求項１７】　前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求項１５に記載の情報処理装置。

【請求項１８】　前記リソースは、装置、情報、または情報に対するライセ

ンスである

ことを特徴とする請求項１５に記載の情報処理装置。

【請求項１９】　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置の情報処理方法において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とする情報処理方法。

【請求項２０】　ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置に実行させるプログラムにおいて、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とするプログラム。

【請求項２１】　電子バリューを管理する情報処理装置において、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込み手段と、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信手段と

を備えることを特徴とする情報処理装置。

【請求項２２】　前記第１または第２の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えることを特徴とする請求項２１に記載の情報処理装置。

【請求項２３】　前記第１と第２の親機の電子バリューを記憶する記憶手段をさらに備え、

前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求項２１に記載の情報処理装置。

【請求項２４】　前記電子バリュー振込み手段は、前記第２の親機から電子バリューを取得し、その電子バリューを前記第１の親機に送信することにより、前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求項２１に記載の情報処理装置。

【請求項２５】　前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項２１に記載の情報処理装置。

【請求項２６】　電子バリューを管理する情報処理装置の情報処理方法において、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信ステップと

を含むことを特徴とする情報処理方法。

【請求項２７】　電子バリューを管理する情報処理装置に実行させるプログラムであって、

ユーザにより操作される端末にリソースを提供する第１の親機に対する、その

リソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラムに関し、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のままユーザの嗜好に合わせた操作性で操作させることができるようにした情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラムに関する。

【０００２】

【従来の技術】

近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の装置を携帯し、屋外で、あるいは移動先においてネットワークに接続してネットワークを介する通信を行なっている。

【０００３】

ここで、既存のインフラを利用したシステムとして、すでに存在する様々な通信網を適宜切り替えて利用するパーソナル通信サービス分散システムが提案されている（例えば特許文献１）。このシステムは、例えば電子メールサービスや電話サービス等の異なるネットワーク通信網を統合して利用することを可能としたシステムである。

【０００４】

しかしながら、ユーザが外出中のような状況で、出先に有るたまたま身近な機器を、自らの所有する同種機種と同じ感覚で利用することはセキュリティやプラ

イバシ等の問題があり、実現されていなかった。

【０００５】

【特許文献１】

特開平８－５６２６３号公報

【０００６】

【発明が解決しようとする課題】

そこで、ユーザが匿名のまま、他者に所有管理されるリソースを所有者との間で相互の信頼関係に基づくセッションを構築し、その上で自らの管理する嗜好情報にしたがって制御することが提案されている。

【０００７】

しかしながら、この方法では、一方的に他者のリソースを使い続けるユーザや、他者のリソースを使う機会が少ないにもかかわらず、自ら所有するリソースを提供し続けるユーザがいる場合、需給のバランスがとれなくなる恐れがある。

【０００８】

そこで、ユーザが、他者の所有するリソースを利用するために必要な対価を、自分と他者の対価を管理する装置を介して支払うシステムが提案されている。

【０００９】

このとき、ユーザが対価を管理する装置と直接アクセスすることによって、ユーザの匿名性を確保することが考えられる。

【００１０】

しかしながら、ここで確保されるユーザの匿名性は、利用シーン（リソースを利用しているとき）の匿名性だけであり、ユーザの個人情報は対価を管理する装置に管理される。従って、ユーザが匿名のまま対価を支払い、他者の所有するリソースを利用することは困難であった。

【００１１】

また、対価を前提に公共の場で通信サービスを行っている無線LAN（Local Area Network）等の事業者とのシームレスなサービスをユーザに提供することは困難であった。

【００１２】

本発明は、このような状況に鑑みてなされたものであり、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにするものである。

【００１３】

【課題を解決するための手段】

本発明の情報処理システムは、ユーザにより操作される端末と、リソースを提供する第１の親機と、ユーザの個人情報を記憶する第２の親機と、電子バリューを管理するバリュー装置とを備える情報処理システムであって、端末は、第１の親機が提供するリソースを要求する信号を、第２の親機に送信するリソース要求信号送信手段と、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する第１の利用権取得手段とを有し、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用し、第１の親機は、リソースの提供に対する対価としての電子バリューが、第２の親機から第１の親機に振り込まれたことの振込み通知を、バリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、第２の親機に対して、利用権を発行する利用権発行手段とを有し、端末が、利用権を提示した場合に、自身が有するリソースの利用を許可し、第２の親機は、端末装置から送信されてくる、リソースを要求する信号に応じて、第１の親機への電子バリューの振込みを、バリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、第１の親機が発行する利用権を取得する第２の利用権取得手段と、第２の利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを有し、バリュー装置は、第２の親機からの要求に応じて、第１の親機に電子バリューを振り込む電子バリュー振込み手段と、第１の親機への電子バリューの振込み通知を、第１の親機に送信する振込み通知送信手段とを有することを特徴とする。

【００１４】

本発明の第１の情報処理装置は、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信手段と、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得手段とを備え、利用権を、第１の親機に提

示して、第１の親機が提供するリソースを利用することを特徴とする。

【００１５】

第２の親機との間で、ユーザが第２の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

【００１６】

リソース要求信号送信手段と利用権取得手段は、第１の親機を介して、第２の親機とやりとりするようにすることができる。

【００１７】

リソース要求信号送信手段と利用権取得手段は、第２の親機との間で、データを暗号化してやりとりするようにすることができる。

【００１８】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００１９】

本発明の第１の情報処理装置の情報処理方法は、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得ステップとを含み、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用することを特徴とする。

【００２０】

本発明の第１の情報処理装置のプログラムは、リソースを提供する第１の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップと、第１の親機が提供するリソースを利用する利用権を、第２の親機から取得する利用権取得ステップとを含み、利用権を、第１の親機に提示して、第１の親機が提供するリソースを利用することを特徴とする。

【００２１】

本発明の第２の情報処理装置は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段とを備え、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

【００２２】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【００２３】

振込み通知が正当であることの認証を行う認証手段をさらに備えるようにすることができる。

【００２４】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００２５】

本発明の第２の情報処理装置の情報処理方法は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

【００２６】

本発明の第２の情報処理装置のプログラムは、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得

した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

【００２７】

本発明の第３の情報処理装置は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを備えることを特徴とする。

【００２８】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【００２９】

端末との間で、ユーザが個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

【００３０】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００３１】

本発明の第３の情報処理装置の情報処理方法は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

【００３２】

本発明の第３の情報処理装置のプログラムは、端末からの要求に応じて、端末

にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

【００３３】

本発明の第４の情報処理装置は、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込み手段と、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信手段とを備えることを特徴とする。

【００３４】

第１または第２の親機との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【００３５】

第１と第２の親機の電子バリューを記憶する記憶手段をさらに備え、電子バリュー振込み手段は、記憶手段に記憶された電子バリューを書き換えることにより、第２の親機から第１の親機に対して、電子バリューを振り込むようにすることができる。

【００３６】

電子バリュー振込み手段は、第２の親機から電子バリューを取得し、その電子バリューを第１の親機に送信することにより、第２の親機から第１の親機に対して、電子バリューを振り込むようにすることができる。

【００３７】

本発明の第４の情報処理装置の情報処理方法は、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの

要求に応じて行う電子バリュー振込みステップと、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

【００３８】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００３９】

本発明の第４の情報処理装置のプログラムは、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップと、第２の親機から第１の親機への電子バリューの振込みが行われたことを表す振込み通知を、第１の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

【００４０】

本発明においては、端末により、第１の親機が提供するリソースを要求する信号が、第２の親機に送信され、記第１の親機が提供するリソースを利用する利用権が、第２の親機から取得される。そして、利用権が、第１の親機に提示され、第１の親機が提供するリソースが利用される。また、第１の親機により、リソースの提供に対する対価としての電子バリューが、第２の親機から第１の親機に振り込まれたことの振込み通知が、バリュー装置から受信され、振込み通知に応じて、第２の親機に対して、利用権が発行される。また、第１の親機により、端末により利用権が提示された場合に、自身が有するリソースの利用が許可される。第２の親機により、端末装置から送信されてくる、リソースを要求する信号に応じて、第１の親機への電子バリューの振込みが、バリュー装置に要求され、電子バリューの振込みに応じて、第１の親機が発行する利用権が取得される。また、第２の親機により、取得された利用権が、端末に提供される。バリュー装置により、第２の親機からの要求に応じて、第１の親機に電子バリューが振り込まれ、第１の親機への電子バリューの振込み通知が、第１の親機に送信される。

【００４１】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。

【００４２】

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

【００４３】

請求項１に記載の情報処理システムは、ユーザにより操作される端末（例えば、図１の移動端末装置１１－２）と、リソースを提供する第１の親機（例えば、図１の親機１２－１）と、前記ユーザの個人情報を記憶する第２の親機（例えば、図１の親機１２－２）と、電子バリューを管理するバリュー装置（例えば、図１のバリュー発行装置１４）とを備え、前記端末は、前記第１の親機が提供するリソースを要求する信号を、前記第２の親機に送信するリソース要求信号送信手段（例えば、図１９のステップＳ２０９の処理を実行するCPU６１）と、前記第１の親機が提供するリソースを利用する利用権（例えば、リソース利用権）を、前記第２の親機から取得する第１の利用権取得手段（例えば、図１９のステップＳ２１０の処理を実行するCPU６１）とを有し、前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用し（例えば、図１９のス

テップＳ２１１，Ｓ２１２の処理を実行するCPU６１）、前記第１の親機は、前記リソースの提供に対する対価としての電子バリューが、前記第２の親機から前記第１の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段（例えば、図１９のステップＳ２６５の処理を実行する親機１２－１のCPU１１１）と、前記振込み通知に応じて、前記第２の親機に対して、前記利用権を発行する利用権発行手段（例えば、図１９のステップＳ２６８の処理を実行する親機１２－１のCPU１１１）とを有し、前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し（例えば、図９のステップＳ８３，Ｓ８４の処理）、前記第２の親機は、前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第１の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振込み要求手段（例えば、図１９のステップＳ３１８の処理を実行する親機１２－２のCPU１１１）と、前記電子バリューの振込みに応じて、前記第１の親機が発行する前記利用権を取得する第２の利用権取得手段（例えば、図１９のステップＳ３２１の処理を実行する親機１２－２のCPU１１１）と、前記第２の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段（例えば、図１９のステップＳ３２４の処理を実行する親機１２－２のCPU111）とを有し、前記バリュー装置は、前記第２の親機からの要求に応じて、前記第１の親機に前記電子バリューを振り込む電子バリュー振込み手段（例えば、図１６のステップＳ１６７の処理を実行するバリュー発行部１３５）と、前記第１の親機への前記電子バリューの振込み通知を、前記第１の親機に送信する振込み通知送信手段（例えば、図１９のステップＳ３４４の処理を実行するバリュー発行部１３５）とを有することを特徴とする。

【００４４】

請求項２に記載の情報処理装置は、リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信手段（例えば、図１９のステップＳ２０９の処理を実行するCPU６１）と、前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得手段（例えば、図１９のステップＳ２１

０の処理を実行するCPU６１）とを備え、前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する（図１９のステップＳ２１１，Ｓ２１２の処理）ことを特徴とする。

【００４５】

前記第２の親機との間で、前記ユーザが前記第２の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段（例えば、図１９のステップＳ２０５乃至ステップＳ２０８の処理を実行するCPU６１）をさらに備えるようにすることができる。

【００４６】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第１の親機を介して、前記第２の親機とやりとりするようにすることができる。

【００４７】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第２の親機との間で、データを暗号化してやりとりするようにすることができる。

【００４８】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００４９】

請求項７に記載の情報処理方法、および請求項８に記載のプログラムは、リソースを提供する第１の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第２の親機に送信するリソース要求信号送信ステップ（例えば、図１９のステップＳ２０９）と、前記第１の親機が提供するリソースを利用する利用権を、前記第２の親機から取得する利用権取得ステップ（例えば、図１９のステップＳ２１０）とを含み、前記利用権を、前記第１の親機に提示して、前記第１の親機が提供するリソースを利用する（図１９のステップＳ２１１，Ｓ２１２の処理）ことを特徴とする。

【００５０】

請求項９に記載の情報処理装置は、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの

振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段（例えば、図１９のステップＳ２６５の処理を実行する親機１２－１のCPU１１１）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段（例えば、図１９のステップＳ２６８の処理を実行する親機１２－１のCPU１１１）とを備え、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図９のステップＳ８３，Ｓ８４の処理）ことを特徴とする。

【００５１】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【００５２】

前記振込み通知が正当であることの認証を行う認証手段（例えば、図１９のステップＳ２６６，Ｓ２６７の処理を実行する親機１２－１のCPU１１１）をさらに備えるようにすることができる。

【００５３】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００５４】

請求項１３に記載の情報処理方法、請求項１１に記載の記録媒体、および請求項１４に記載のプログラムは、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップ（例えば、図１９のステップＳ２６５）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップ（例えば、図１９のステップＳ２６８）とを含み、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図９のステップＳ８３，Ｓ８４の処理）ことを特徴とする。

【００５５】

請求項１５に記載の情報処理装置は、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段（例えば、図１９のステップＳ３１８の処理を実行する親機１２－２のCPU１１１）と、前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段（例えば、図１９のステップＳ３２１の処理を実行する親機１２－２のCPU１１１）と、前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段（例えば、図１９のステップＳ３２４の処理を実行する親機１２－２のCPU１１１）とを備えることを特徴とする。

【００５６】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図１９のステップＳ３１９，Ｓ３２０の処理を実行する親機１２－２のCPU１１１）をさらに備えるようにすることができる。

【００５７】

前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段（例えば、図１９のステップＳ３１１乃至ステップＳ３１４の処理を実行する親機１２－２のCPU１１１）をさらに備えるようにすることができる。

【００５８】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００５９】

請求項１９に記載の情報処理方法、および請求項２０に記載のプログラムは、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップ（例えば、図１９のステップＳ３１８）と、前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステ

ップ（例えば、図１９のステップＳ３２１）と、前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップ（例えば、図１９のステップＳ３２４）とを含むことを特徴とする。

【００６０】

請求項２１に記載の情報処理装置は、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込み手段（例えば、図１６のステップＳ１６７の処理を実行するバリュー発行部１３５）と、前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信手段（例えば、図１９のステップＳ３４４の処理を実行するバリュー発行部１３５）とを備えることを特徴とする。

【００６１】

前記第１または第２の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図１９のステップＳ３４２，Ｓ３４３の処理を実行する共通秘密鍵認証部１３３）をさらに備えるようにすることができる。

【００６２】

前記第１と第２の親機の電子バリューを記憶する記憶手段（例えば、図１５のバリュー記憶部１４０）をさらに備え、前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込むようにすることができる。

【００６３】

前記電子バリュー振込み手段は、前記第２の親機から電子バリューを取得し、その電子バリューを前記第１の親機に送信することにより、前記第２の親機から前記第１の親機に対して、前記電子バリューを振り込むようにすることができる。

【００６４】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【００６５】

請求項２６の情報処理方法、および請求項２７のプログラムにおいて、ユーザにより操作される端末にリソースを提供する第１の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第２の親機からの要求に応じて行う電子バリュー振込みステップ（例えば、図１６のステップＳ１６７）と、前記第２の親機から前記第１の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第１の親機に送信する振込み通知送信ステップ（例えば、図１９のステップＳ３４４）とを含むことを特徴とする。

【００６６】

図１は、本発明を適用した情報処理システム１の構成例を示すブロック図である。この情報処理システム１では、親機１２とバリュー発行装置１４間の処理を安全確実に行うために用いられた公開鍵暗号（PKI（Public Key Infrastructure））系の暗号技術を用いてセキュリティを確保する。

【００６７】

図１の例においては、２人のユーザが、それぞれ移動端末装置１１－１と移動端末装置１１－２を有している。ユーザは、必ず１つの親機にユーザの個人情報（利用履歴、嗜好、決済関連等）を格納し、ユーザの認証情報として共通秘密鍵を取得する。この例では、ユーザと親機が共通秘密鍵として同じパスフレーズを有しており、ユーザと親機は、同じパスフレーズを有することを確認することで、ユーザを認証する。

【００６８】

また、この例では、移動端末装置１１－１のユーザは親機１２－１に、移動端末装置１１－２のユーザは親機１２－２に、ユーザの個人情報を格納している。

【００６９】

さらに、移動端末装置１１－１は、その移動端末装置１１－１のユーザの個人情報を格納した親機１２－１と直接無線で通信可能な位置にあり、移動端末装置

１１－２は、その移動端末装置１１－２のユーザの個人情報を格納した親機１２－２とは遠隔地に設置された、親機１２－１と直接無線で通信できる位置にある。従って、移動端末装置１１－２は、親機１２－２とは無線で通信することが困難であるが、親機１２－１とは直接無線で通信できる。

【００７０】

移動端末装置１１－１と移動端末装置１１－２は、ユーザとともに移動し、無線通信を用いてユーザからの指示に対応する信号を親機１２－１に送信する。また、移動端末装置１１－１と移動端末装置１１－２は、無線通信を用いて、親機１２－１からの信号を受信する。

【００７１】

以下、移動端末装置１１－１と移動端末装置１１－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、移動端末装置１１と称する。

【００７２】

この移動端末装置１１とユーザとは、依存関係がなく、ユーザが移動端末装置１１を利用するときにのみ、移動端末装置１１は、ユーザの認証を行う。従って、移動端末装置１１には、ユーザの認証情報の入力機能が備えられている。

【００７３】

図１の例においては、移動端末装置１１－１および移動端末装置１１－２のユーザは、ユーザの認証情報として、共通秘密鍵３１および共通秘密鍵３２を、それぞれ入力している。

【００７４】

親機１２－１は、所定の空間に配置され、無線通信を用いて、移動端末装置１１から送信された信号を受信するとともに、移動端末装置１１に信号を送信する。また、親機１２－１は、ユーザに提供する情報であるコンテンツ等のリソースを有するリソース機器１５－１、リソース機器１５－２、リソース機器１６－１、およびリソース機器１６－２と接続されている。さらに、親機１２－１は、インターネット２１を介して、認証装置１３およびバリュー発行装置１４と接続されている。

【００７５】

ここで、親機１２－１は、例えば、移動端末装置１１－１のユーザのユーザ宅の、いわゆるホームサーバで構成することができる。同様に、親機１２－２も、例えば、移動端末装置１１－２のユーザのユーザ宅のホームサーバで構成することができる。

【００７６】

以下、リソース機器１５－１とリソース機器１５－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器１５と称する。また、リソース機器１６－１とリソース機器１６－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器１６と称する。

【００７７】

これにより、移動端末装置１１は、親機１２－１を介して、親機１２－１に接続されたリソース機器１５、リソース機器１６、およびインターネット２１を介して接続された機器との通信ができる。

【００７８】

また、親機１２－１は、ユーザの認証情報として共通秘密鍵３３を格納している。即ち、この共通秘密鍵３３は、移動端末装置１１－１のユーザに入力された共通秘密鍵３１と等しくなっている。さらに、親機１２－１は、バリュー発行装置１４により送信された共通秘密鍵３４と、自らの正当性を証明する秘密鍵３５を記憶している。

【００７９】

親機１２－２は、インターネット２１を介して、親機１２－１、認証装置１３、およびバリュー発行装置１４と接続されている。

【００８０】

また、親機１２－２は、ユーザの認証情報として共通秘密鍵３６を格納している。この共通秘密鍵３６は、移動端末装置１１－２のユーザに入力された共通秘密鍵３２と等しくなっている。さらに、親機１２－１は、バリュー発行装置１４により送信された共通秘密鍵３７と、自らの正当性を証明する秘密鍵３８を記憶している。

【００８１】

以下、親機１２－１と親機１２－２のそれぞれを個々に区別する必要がない場合、適宜、まとめて、親機１２と称する。

【００８２】

認証装置１３は、親機１２－１の秘密鍵３５に対応する公開鍵３９、親機１２－２の秘密鍵３８に対応する公開鍵４０、およびバリュー発行装置１４の後述する秘密鍵４３に対応する公開鍵４１を記憶する。また、認証装置１３は、自らの正当性を証明する秘密鍵４２を記憶する。

【００８３】

認証装置１３は、他の装置からの要求に応じて公開鍵を検索し、その公開鍵を他の装置に送信する。秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。また、認証装置１３は、電子証明書（図１１）の発行および鍵の失効管理を行う。

【００８４】

バリュー発行装置１４は、親機１２－１と親機１２－２に対し、バリュー（電子バリュー）の発行および流通管理を行う。バリュー発行装置１４は、自らの正当性を証明する秘密鍵４３および共通秘密鍵４４を記憶している。バリュー発行装置１４は、共通秘密鍵４４をバリューを発行する相手である親機１２－１と親機１２－２に送信し、親機１２－１に共通秘密鍵３４として記憶させるとともに、親機１２－２に共通秘密鍵３７として記憶させる。即ち、共通秘密鍵３４、共通秘密鍵３７、および共通秘密鍵４４は等しい。

【００８５】

ユーザは、自身の個人情報（利用履歴、嗜好、決済関連情報等）を自身の親機にのみ格納し、共通秘密鍵を取得する。そして、この共通秘密鍵を用いて、全ての通信を行うことにより、ユーザは、匿名性を保ち、安全に通信を行うことができる。

【００８６】

なお、上述の例では、２個の移動端末装置が存在するが、移動中のユーザが多数いる場合、その数だけの移動端末装置が存在するものとする。また、上述の例では、２個の親機が存在するが、各空間には、それぞれの空間に必要な数だけの

親機が存在するものとする。

【００８７】

また、共通秘密鍵３１と共通秘密鍵３２は、移動端末装置１１のユーザを認証するための鍵である。共通秘密鍵３４、共通秘密鍵３７、および共通秘密鍵４４は、バリューを扱う正当な装置であることを認証するための鍵である。秘密鍵３５、秘密鍵３８、および秘密鍵４３は、自らの正当性を証明するための鍵であり、装置間における通信中の改ざんを防止する。

【００８８】

以上のように構成される通信システム１によって、例えば、移動端末装置１１－２のユーザがその個人情報を記憶していない親機１２－１のリソースを利用する場合には、移動端末装置１１－２は、親機１２－１の利用したいリソースを指定し、個人情報を記憶している親機１２－２に、そのリソースの利用を要求する。親機１２－２は、移動端末装置１１－２からリソースが要求されると、親機１２－１に対するリソース利用に必要なバリューの支払いを、バリュー発行装置１４に要求する。

【００８９】

バリュー発行装置１４は、親機１２－２のバリューを親機１２－１に移動させ、親機１２－１にバリューの振込みが行われたことを表す振込み通知を発行する。親機１２－１は、バリュー発行装置１４から振り込み通知を受信すると、親機１２－２にリソースを利用する利用権を発行する。親機１２－２は、親機１２－１から利用権が発行されると、その利用権を移動端末装置１１－２に送信する。移動端末装置１１－２は、その利用権を親機１２－１に提示し、リソースを要求する。親機１２－２は、移動端末装置１１－２から利用権を提示された場合、リソースの利用を許可する。

【００９０】

次に、図２は、図１の移動端末装置１１の詳細構成例を示している。

【００９１】

図２の例では、移動端末装置１１－１を説明するが、移動端末装置１１－２も同様に構成される。

【００９２】

移動端末装置１１－１は、CPU (Central Processing Unit) ６１、ROM(Read Only Memory)６２、RAM(Random Access Memory)６３、表示部６４、リーダライタ６５、送信部６６、アンテナ６７、受信部６８、暗号/復号部６９、および操作入力部７０から構成される。

【００９３】

なお、移動端末装置１１－１のユーザは、あらかじめ取得した共通秘密鍵３１、自身の親機１２－１が接続しているリソースの情報、および自身の親機１２－１のネットワーク上のアドレスを格納した非接触ＩＣ（Integrated Circuit）カード７１を有している。

【００９４】

このように、共通秘密鍵３１を改ざんが困難な非接触ＩＣカードに安全に格納することにより、通信システムの安全性と利便性を向上させることができる。また、非接触ＩＣカードは、非接触のインターフェースであるので、利用時の利便性が向上し、かつ簡単な操作で処理が可能になる。

【００９５】

この非接触ＩＣカードとしては、例えば、FeliCa（商標）のような対タンパ性の高いＩＣチップが用いられる。なお、共通秘密鍵３１などは、非接触型ではなく接触型のデバイスに格納することも可能である。但し、便利性やデバイスの劣化に対する耐性を考えると、接触型ではなく、非接触型を採用するのが望ましい。

【００９６】

CPU６１は、ROM６２に記憶されているプログラムに従って各種の処理を実行する。RAM６３には、CPU６１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【００９７】

表示部６４は、CPU６１からの指令により、例えば、移動端末装置１１－１が利用できるリソースの情報を表示する。リーダライタ６５は、ユーザが有する非接触ＩＣカード７１に封じ込められた（格納された）共通秘密鍵３１、ユーザの

個人情報を記憶した親機１２－１が接続しているリソースの情報、および個人情報を記憶した親機１２－１のネットワーク上のアドレスを読み込み、CPU６１に共通秘密鍵３１、リソース情報、およびアドレスを供給する。ここで、また、リーダライタ６５は、CPU６１からの指令により、必要に応じて非接触ＩＣカード７１にデータを書き込む。

【００９８】

送信部６６は、CPU６１からの指令により、親機１２－１に送信する信号をアンテナ６７に供給する。アンテナ６７は、送信部６６から供給された信号を、無線通信を用いて親機１２－１に送信する。さらに、アンテナ６７は、親機１２－１から送信された信号を受信し、その信号を受信部６８に供給する。受信部６８は、アンテナ６７から供給された信号を、CPU６１に供給する。

【００９９】

暗号/復号部６９は、非接触ＩＣカード７１から読み込まれた共通秘密鍵３１を暗号化したり、受信部６８で受信した暗号化された共通秘密鍵を復号し、その復号した共通秘密鍵をさらに暗号化する。操作入力部７０は、ユーザにより操作され、その操作に対応する信号がCPU６１に供給される。

【０１００】

図３は、図２の移動端末装置１１がリソースを取得する処理を説明するフローチャートである。なお、ユーザは、予め個人情報を自身の親機に格納しており、共通秘密鍵３１（３２）、その親機に接続されているリソースの情報、およびその親機のネットワーク上のアドレスは非接触ＩＣカード７１に記憶されているものとする。図３の処理は、例えば、ユーザが操作入力部７０を操作して親機１２－１に接続されているリソースの取得を要求したときに開始される。

【０１０１】

ステップＳ１において、CPU６１は、移動端末装置１１を使用するユーザの個人情報が格納されている自身の親機（以下、適宜、本親機と称する）と無線通信が可能であるかどうかを判定する。例えば、移動端末装置１１は、無線通信が可能な機器を検索し、検索された機器の中に本親機が含まれているかどうかを判定する。

【０１０２】

ステップＳ１で、CPU６１は、本親機と無線通信が可能であると判定した場合、ステップＳ２に進み、CPU６１は、本親機（例えば、移動端末装置１１－１の場合、親機１２－１）との間で共通秘密鍵認証処理を行ない、ステップＳ３に進む。この共通秘密鍵認証処理の詳細は、図４で後述する。

【０１０３】

ステップＳ３では、CPU６１は、ユーザが操作入力部７０を操作することにより指定したリソースを要求する信号を、送信部６６を制御して、アンテナ６７から本親機である、例えば、親機１２－１に送信する。即ち、ユーザは、非接触ＩＣカード７１に記憶され、リーダライタ６５から読み込まれたリソース情報を表示部６４に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを要求する信号がアンテナ６７から送信される。なお、以下の説明では、CPU６１が送信部６６を制御して、信号を送信することを、単に、CPU６１が信号を送信するという。

【０１０４】

ステップＳ３の処理後は、ステップＳ４に進み、アンテナ６７は、ステップＳ３のリソース要求信号に対応して親機１２－１から送信されたリソース（を使用するのに必要な情報）を受信し、受信部６８を介してCPU６１に供給する。そして、CPU６１は、そのリソースをRAM６３に保持する。なお、以下の説明では、アンテナ６７が信号を受信し、受信部６８を介して、CPU６１にその信号を供給することを、単に、CPU６１が信号を受信するという。

【０１０５】

一方、ステップＳ１で、CPU６１は、本親機と無線通信が可能ではないと判定した場合（例えば、移動端末装置１１－２が、親機１２－２と通信できない場合）、ステップＳ５に進み、リソース情報取得処理を行ない、ステップＳ６に進む。即ち、例えば、移動端末装置１１－２については、現在、その移動端末装置１１－２と通信できる親機１２－１が本親機ではないので、移動端末装置１１－２は、親機１２－１が接続しているリソースの情報を非接触ＩＣカード７１に記憶していない。従って、移動端末装置１１－２は、親機１２－１が接続しているリ

ソースの情報を取得する必要があり、このため、ステップＳ５において、リソース情報取得処理が行なわれる。このリソース情報取得処理の詳細は、図５で後述する。

【０１０６】

ステップＳ６において、CPU６１は、本親機（親機１２－２）との間で共通秘密鍵認証処理を行い、ステップＳ７に進む。なお、いまの場合、移動端末装置１１－２は、本親機である親機１２－２と直接無線通信することはできないため、ステップＳ６の共通秘密鍵認証処理は、後述するように、移動端末装置１１－２と親機１２－２との間で、親機１２－１およびインターネット２１を介した通信を行うことにより実行される。この共通秘密鍵認証処理の詳細は、図４で後述する。

【０１０７】

ステップＳ７では、CPU６１は、非接触ＩＣカード７１から、親機１２－２のアドレスを読み出す。そして、ユーザが操作入力部７０を操作することにより指定したリソースを要求する信号（リソース利用権発行要求）を親機１２－２のアドレスとともに、親機1２－１に送信し、インターネット２１経由で親機１２－２に送信する。即ち、ユーザは、ステップＳ５で取得した親機１２－１が接続しているリソースのリソース情報を表示部６４に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを利用する権利を要求する信号として、リソース利用権発行要求が、移動端末装置１１－２から、親機１２－１およびインターネット２１を介して、本親機である親機１２－２に送信される。

【０１０８】

ここで、移動端末装置１１－２は、上述のように、親機１２－２のアドレスを親機１２－１に知らせる。これにより、移動端末装置１１－２は、無線通信可能な親機１２－１とインターネット２１を介して、本親機である親機１２－２と通信が可能になる。

【０１０９】

ステップＳ７の処理後は、ステップＳ８に進み、CPU６１は、親機１２－１か

ら、リソースを取得する権利を記載した権利文のデータであるリソース利用権を受信したか否かを判定する。ステップＳ８で、CPU６１は、親機１２－１から権利文を受信したと判定した場合、移動端末装置１１－２は、親機１２－１に接続しているリソースを利用する権利があるので、ステップＳ９に進み、親機１２－１に、受信した権利文とリソース要求信号を送信する。ステップＳ９の処理後は、ステップＳ１０に進み、CPU６１は、リソース要求信号に対応して、親機１２－１から送信されたリソース（を利用するのに必要な情報）を受信し、そのリソースをRAM６３に保持して、処理を終了する。

【０１１０】

この場合、移動端末装置１１－２は、本親機でない親機１２－１のリソースを使用することができる。

【０１１１】

一方、ステップＳ８で、CPU６１は、親機１２－１から権利文を受信していないと判定した場合、ステップＳ１１に進み、親機１２－２から、親機１２－１を介して、リソースを取得する権利を記載した権利文を発行できないことを示すエラー通知を受信したか否かを判定する。ステップＳ１１で、CPU６１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ８に戻り、上述した処理を繰り返す。

【０１１２】

また、ステップＳ１１において、CPU６１は、親機１２－２からエラー通知を受信したと判定した場合、移動端末装置１１－２は、親機１２－１に接続しているリソースを取得する権利がないので、処理を終了する。

【０１１３】

図４は、図３のステップＳ２とステップＳ６の共通秘密鍵認証処理を説明するフローチャートである。この処理は、移動端末装置１１とそのユーザの本親機との間で行われる。

【０１１４】

図４の例では、移動端末装置１１－１における共通秘密鍵認証処理を説明するが、移動端末装置１１－２における場合も同様の処理が行われる。但し、移動端

末装置１１－２の場合は、本親機である親機１２－２と無線通信が可能ではないので、無線通信可能な親機１２－１にその本親機である親機１２－２のアドレスを通知し、親機１２－１を介して、インターネット２１経由で本親機である親機１２－２と通信する。

【０１１５】

ステップＳ２１において、CPU６１は、リーダライタ６５を制御して、非接触ＩＣカード７１から、ユーザの認証情報である共通秘密鍵３１を読み込み、RAM６３に保持する。ステップＳ２１の処理後は、ステップＳ２２に進み、CPU６１は、共通秘密鍵３１を暗号化し、ステップＳ２３に進む。即ち、移動端末装置１１－１は、認証装置１３から親機１２－１（本親機）の秘密鍵３５に対応する公開鍵３９を取得し、RAM６３に保持する。CPU６１は、RAM６３に保持した公開鍵３９を、共通秘密鍵３１とともに暗号/復号部６９に供給する。暗号/復号部６９は、その公開鍵３９を用いて、共通秘密鍵３１を暗号化する。

【０１１６】

ステップＳ２３では、CPU６１は、ステップＳ２２で暗号化した共通秘密鍵３１を、本親機である親機１２－１に送信し、ステップS２４に進む。ステップＳ２４において、CPU６１は、親機１２－１（本親機）から、後述する図８のステップＳ６４で送信されてくる秘密鍵３５で暗号化された共通秘密鍵３３を受信したかどうかを判定し、暗号化された共通秘密鍵３３を受信していないと判定した場合、受信されるまで待機する。

【０１１７】

ステップＳ２４において、CPU６１は、親機１２－１から暗号化された共通秘密鍵３３を受信したと判定した場合、ステップＳ２５に進み、暗号/復号部６９を制御し、その暗号化された共通秘密鍵３３を、ステップＳ２２の処理でRAM６３に保持した、秘密鍵３５と対の公開鍵３９を用いて復号する。このとき、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて生成された暗号文（パスフレーズ）を他方の鍵を用いて復号できる関係にあるので、秘密鍵３５に基づいて暗号化された共通秘密鍵３３（パスフレーズ）が、親機１２－１から送信され、移動端末装置１１－１で受信されるまでの間に改ざんされなかった場合、

その暗号化された共通秘密鍵３３は、公開鍵３９に基づいて復号されると、共通秘密鍵３３となる。

【０１１８】

ステップＳ２５の処理後は、ステップＳ２６に進み、CPU６１は、暗号/復号部６９を制御して、復号した共通秘密鍵３３を、ステップＳ２２の処理でRAM６３に保持した公開鍵３９を用いて暗号化し、その暗号化した共通秘密鍵を親機１２－１（本親機）に送信し、ステップＳ２７に進む。ステップＳ２７において、CPU６１は、親機１２－１（本親機）から、後述する図８のステップＳ６８の処理で秘密鍵３５を用いて暗号化された共通秘密鍵（親機１２－１が、ステップＳ２３で親機１２－１に送信された暗号化した共通秘密鍵３１を秘密鍵３５を用いて復号し、さらに暗号化した共通秘密鍵）３１を受信したかどうかを判定する。

【０１１９】

ステップＳ２７で、CPU６１は、親機１２－１から暗号化された共通秘密鍵３１を受信したと判定した場合、ステップＳ２８に進み、暗号/復号部６９を制御して、その暗号化された共通秘密鍵３１を、秘密鍵３５と対のRAM６３に保持した公開鍵３９を用いて復号する。ステップＳ２８の処理後は、ステップＳ２９に進み、ステップＳ２８で復号された共通秘密鍵が、ステップＳ２１でRAM６３に保持された共通秘密鍵３１と等しいかどうかを判定する。

【０１２０】

ステップＳ２９において、CPU６１は、復号された共通秘密鍵３１が、RAM６３に保持された共通秘密鍵３１と等しいと判定した場合、図３のステップＳ３または図３のステップＳ７にリターンする。即ち、この場合、ステップＳ２３で公開鍵３９を用いて暗号化された共通秘密鍵３１が、親機１２－１により秘密鍵３５を用いて正常に復号され、共通秘密鍵３１が得られている。そして、その共通秘密鍵３１が、親機１２－１において秘密鍵３５を用いて暗号化され、その暗号化された共通秘密鍵３１が、移動端末装置１１－１において、公開鍵３９を用いて正常に復号され、共通秘密鍵３１が得られている。

【０１２１】

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号

化された共通秘密鍵３１を他方の鍵を用いて復号できる関係にあるので、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことを認識できる。

【０１２２】

一方、ステップＳ２９において、CPU６１は、ステップＳ２８で復号された共通秘密鍵が、RAM６３に保持された共通秘密鍵３１と等しくないと判定した場合、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて生成された共通秘密鍵３１を他方の鍵を用いて復号できる関係にないので、移動端末装置１１－１と親機１２－１が通信する間で改ざんがあった、あるいは、親機１２－１が正当な装置でないと認識し、処理を終了する。

【０１２３】

このように、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと認識できたときのみ、図３のステップＳ３または図３のステップＳ７に進み、親機１２－１にリソースを要求する信号を送信するので、移動端末装置１１－１と親機１２－１の両者間での通信中のデータ秘匿が可能となる。

【０１２４】

一方、ステップＳ２７において、CPU６１は、親機１２－１から暗号化された共通秘密鍵３１を受信していないと判定した場合、ステップＳ３０に進み、後述する図８のステップＳ７１で親機１２－１が送信した、親機１２－１と移動端末装置１１－１の関係が正当ではないことを示すエラー通知を受信したか否かを判定する。ステップＳ３０において、CPU６１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ２７に戻り、上述した処理を繰り返す。

【０１２５】

一方、ステップＳ３０において、CPU６１は、親機１２－１からエラー通知を受信したと判定した場合、親機１２－１と移動端末装置１１－１の関係は正当ではないので、処理を終了する。

【０１２６】

図５は、図３のステップＳ５の処理を説明するフローチャートである。

【０１２７】

ステップＳ４１において、例えば、移動端末装置１１－２のCPU６１は、直接無線通信することができる本親機でない親機１２－１にブロードキャストを要求する。即ち、移動端末装置１１－２は、ブロードキャスト要求（デバイス探索）等によって、親機１２－１が管理する機器（例えば、リソース機器１５－１等）や電子権利などのリソース情報を取得する。

【０１２８】

ステップＳ４１の処理後は、ステップＳ４２に進み、CPU６１は、親機１２－１から、ブロードキャスト要求を許可された（後述する図１２のステップＳ１２１で送信されたブロードキャスト要求許可の通知を受信した）かどうかを判定する。ステップＳ４２において、CPU６１は、親機１２－１からブロードキャスト要求が許可されたと判定した場合、ステップＳ４３に進み、親機１２－１にリソース情報を要求する。

【０１２９】

ステップＳ４３の処理後は、ステップＳ４４に進み、CPU６１は、リソース情報要求に対応して、親機１２－１から送信されたリソース情報を受信し、そのリソース情報をRAM６３に保持する。

【０１３０】

一方、ステップＳ４２において、CPU６１は、親機１２－１から、ブロードキャスト要求を許可されていないと判定した場合、ステップＳ４５に進み、ブロードキャスト要求に対応して親機１２－１から送信されたブロードキャスト要求の不許可を示すエラー通知が、受信されたかどうかを判定する。ステップＳ４５において、CPU６１は、エラー通知が受信されていないと判定した場合、ステップＳ４２に戻り、上述した処理を繰り返す。

【０１３１】

また、ステップＳ４５において、CPU６１は、エラー通知が受信されたと判定した場合、親機１２－１にブロードキャスト要求が許可されず、親機１２－１からリソース情報を得ることができないので、処理を終了する。

【０１３２】

図６は、図１の親機１２の詳細構成例を示している。

【０１３３】

図６の例では、親機１２－１を説明するが、親機１２－２も同様に構成される。

【０１３４】

親機１２－１は、CPU９１、ROM９２、RAM９３、アンテナ９４、受信部９５、送信部９６、入出力部９７、データバス９８、リソース制御部９９、および通信部１００から構成されている。

【０１３５】

CPU９１は、ROM９２に記憶されているプログラムに従って各種の処理を実行する。例えば、CPU９１は、受信部９５から供給された受信データの供給先を判定し、入出力部９７を制御して、その供給先に、受信データを供給する。RAM９３には、CPU９１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【０１３６】

アンテナ９４は、移動端末装置１１から送信された信号を受信し、その信号を受信部９５に供給する。また、アンテナ９４は、送信部９６から供給された信号を移動端末装置１１に送信する。

【０１３７】

受信部９５は、アンテナ９４から供給された信号をCPU９１に供給する。送信部９６は、CPU９１からの指令に基づいて、移動端末装置１１に送信する信号をアンテナ９４に供給する。

【０１３８】

入出力部９７は、データバス９８を介してリソース制御部９９と通信部１００に接続されるとともに、リソース機器１６－１とリソース機器１６－２に接続されている。リソース制御部９９は、リソース機器１５－１とリソース機器１５－２にそれぞれ接続されている。

【０１３９】

通信部１００は、CPU９１からの指令に基づき、インターンネット２１を介して、親機１２－２、認証装置１３、およびバリュー発行装置１４に信号を送信するとともに、親機１２－２、認証装置１３、およびバリュー発行装置１４から信号を受信する。

【０１４０】

図７は、図６のリソース制御部９９の詳細構成例を示している。

【０１４１】

リソース制御部９９は、CPU１１１、ROM１１２、RAM１１３、入出力部１１４、リーダライタ１１５、表示部１１６、および暗号/復号部１１７から構成される。

【０１４２】

CPU１１１は、ROM１１２に記憶されているプログラムに従って各種の処理を実行する。RAM１１３は、ユーザの個人情報を格納しており、CPU１１１は、個人情報を管理している。また、RAM１１３には、CPU１１１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【０１４３】

CPU１１１は、入出力部１１４を介して、リソース機器１５－１とリソース機器１５－２に接続されており、リソース機器１５－１とリソース機器１５－２から供給されたリソースを、データバス９８および入出力部９７を介して、CPU９１に供給する。リーダライタ１１５は、親機１２－１に備えられた非接触ＩＣカード１２１から、データを読み込んだり、データを書き込む。

【０１４４】

非接触ＩＣカード１２１には、個人認証用の情報の格納領域と電子バリューのための認証用の情報の格納領域が設けられている。個人認証用の情報の格納領域には、移動端末装置１１－１の共通秘密鍵３１と同一の共通秘密鍵３３と自らの正当性を証明するための秘密鍵３５が格納されている。電子バリューのための認証用の情報の格納領域には、バリュー発行装置１４により発行された共通秘密鍵３４等が格納されている。なお、電子バリューのための認証用の情報の格納領域は、認証用と電子バリュー用の領域に分けることができる。認証用の領域には、

秘密鍵３４が格納され、電子バリューの領域には、電子バリュー（例えば、権利文）が格納される。

【０１４５】

このように、共通秘密鍵３３、共通秘密鍵３４、および秘密鍵３５を改ざんが困難な非接触ＩＣカード１２１に安全に格納することにより、通信システムの安全性と利便性を向上させることができる。

【０１４６】

表示部１１６は、CPU１１１の指令により、例えば、リソース情報を表示する。暗号/復号部１１７は、鍵、その他の情報を暗号化または復号する。

【０１４７】

なお、親機１２－１は、物理的に1つの筐体で構成する必要はなく、データバスを経由して複数の機器が協調して機能を実現するように構成してもよい。

【０１４８】

図８は、図７の親機１２のリソース制御部９９がリソースを制御する処理を説明するフローチャートである。この処理は、例えば、移動端末装置１１から信号を受信したとき開始される。

【０１４９】

以下の説明では、親機１２－１がリソースを制御する処理を説明するが、親機１２－２における場合も同様の処理が行われる。

【０１５０】

ステップＳ６１では、CPU１１１は、リーダライタ１１５を制御し、非接触ＩＣカード１２１から共通秘密鍵３３を読み込み、その共通秘密鍵３３をRAM１１３に保持する。ステップＳ６１の処理後は、ステップＳ６２に進み、CPU１１１は、図４のステップＳ２３で移動端末装置１１－１から送信された暗号化した共通秘密鍵３１が受信されたかどうかを判定する。

【０１５１】

即ち、CPU９１は、アンテナ９４により受信され、受信部９５を介して供給された信号が、親機１２－１に対するものである場合、入出力部９７を制御し、データバス９８を介して、その信号をリソース制御部９９のCPU１１１に供給し、C

PU１１１は、その信号が暗号化された共通秘密鍵３１であるかどうかを判定する。なお、以下の説明では、このようにCPU９１がアンテナ９４により受信された信号をリソース制御部９９のCPU１１１に供給することを、単に、CPU１１１が信号を受信するという。

【０１５２】

ステップＳ６２において、CPU１１１は、移動端末装置１１－１から暗号化された共通秘密鍵３１が受信されたと判定した場合、ステップＳ６３に進み、非接触ＩＣカード１２１から秘密鍵３５を読み込み、その暗号化された共通秘密鍵３１と秘密鍵３５をRAM１１３に保持する。そして、CPU１１１は、暗号/復号部１１７を制御し、ステップＳ６１でRAM１１３に保持した共通秘密鍵３３を、秘密鍵３５を用いて暗号化する。

【０１５３】

ステップＳ６３の処理後は、ステップＳ６４に進み、CPU１１１は、ステップＳ６２で暗号化された共通秘密鍵３３を、移動端末装置１１－１に送信し、ステップＳ６４からステップＳ６５に進む。ステップＳ６５では、CPU１１１は、図４のステップＳ２６で移動端末装置１１－１から送信された暗号化された共通秘密鍵が受信されたかどうかを判定し、移動端末装置１１－１から暗号化された共通秘密鍵が受信されるまで待機する。

【０１５４】

ステップＳ６５において、CPU１１１は、移動端末装置１１－１から暗号化された共通秘密鍵が供給されたと判定した場合、ステップＳ６６に進み、その暗号化された共通秘密鍵を復号し、ステップＳ６７に進む。即ち、CPU１１１は、暗号/復号部１１７を制御し、ステップＳ６３でRAM１１３に保持した、公開鍵３９と対の秘密鍵３５を用いて、暗号化された共通秘密鍵を復号する。

【０１５５】

ステップＳ６７では、CPU１１１は、その復号された共通秘密鍵が、RAM１１３に保持された共通秘密鍵３３と等しいかどうかを判定する。ステップＳ６７において、CPU１１１は、その復号された共通秘密鍵がRAM１１３に保持された共通秘密鍵３３と等しいと判定した場合、ステップＳ６８に進む。

【０１５６】

即ち、この場合、ステップＳ６３で秘密鍵３５を用いて暗号化された共通秘密鍵３３が、移動端末装置１１－１において、公開鍵３９を用いて正常に復号され、共通秘密鍵３３が得られている。そして、その秘密鍵３３が移動端末装置１１－１において、公開鍵３９を用いて暗号化され、その暗号化されたた共通秘密鍵３１が、親機１２－１において、秘密鍵３５を用いて正常に復号され、共通秘密鍵３３が得られている。

【０１５７】

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号化された共通秘密鍵３３を他方の鍵を用いて復号できる関係にあるので、親機12－1は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことが認識できる。

【０１５８】

その後、ステップＳ６８において、CPU１１１は、ステップＳ６２で移動端末装置１１－１から受信し、RAM１１３に保持した暗号化された共通秘密鍵３１を、RAM１１３に保持した公開鍵３９と対の秘密鍵３５を用いて復号する。

【０１５９】

ステップＳ６８の処理後は、ステップＳ６９に進み、CPU１１１は、ステップＳ６８で復号した共通秘密鍵が、RAM１１３に保持した共通秘密鍵３３と等しいかどうかを判定する。ステップＳ６９において、CPU１１１は、その復号した共通秘密鍵がRAM１１３に保持した共通秘密鍵３３と等しいと判定した場合、ステップＳ７０に進む。

【０１６０】

即ち、この場合、図４のステップＳ２２で移動端末装置１１－１により公開鍵３９を用いて暗号化された、秘密鍵３３と同一の共通秘密鍵３１が、ステップＳ６８で親機１２－１により秘密鍵３５を用いて正常に復号され、共通秘密鍵３１が得られている。そして、移動端末装置１１－１が有する共通秘密鍵３１と親機12-1が有する共通秘密鍵３３が同一であることが検証、つまり、移動端末装置１１－１のユーザが、親機１２－１のユーザであることが検証されている。

【０１６１】

従って、秘密鍵３５とそれに対応する公開鍵３９は、一方の鍵に基づいて暗号化された共通秘密鍵３１を他方の鍵を用いて復号できる関係にあるので、親機１２－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったことが認識できる。また、移動端末装置１１－１が有する共通秘密鍵３１と親機１２－１が有する共通秘密鍵３３が等しくなっているので、親機１２－１は、移動端末装置１１－１のユーザが個人情報を格納したユーザであることを認識する。

【０１６２】

その後、ステップＳ７０において、暗号/復号部６９を制御して、その復号した共通秘密鍵を、RAM１１３に保持した秘密鍵３５を用いて暗号化し、移動端末装置１１－１に送信する。

【０１６３】

一方、ステップＳ６７において、CPU１１１は、ステップＳ６６で復号された共通秘密鍵がRAM１１３に保持する共通秘密鍵３３と等しくないと判定した場合、またはステップＳ６９で、ステップＳ６８で復号された共通秘密鍵がRAM１１３に保持する共通秘密鍵３３と等しくないと判定した場合、移動端末装置１１－１と親機１２－１が通信する間で改ざんがあったか、または親機１２－１が移動端末装置１１－１の本親機ではないので、ステップＳ７１に進み、移動端末装置１１－１と親機１２－１の関係が正当ではないことを示すエラー通知を送信し、処理を終了する。

【０１６４】

このように、親機１２－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなく、かつ移動端末装置１１－１の本親機であると認識できたときのみ、復号した共通秘密鍵３１を暗号化して移動端末装置１１－１に送信する。

【０１６５】

この後、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと認識できたときのみリソースを要求する信号を親

機１２－１に送信するので、移動端末装置１１－１は、移動端末装置１１－１と親機１２－１が通信する間で改ざんがなかったと移動端末装置１１－１と親機１２－１の両者で認識（双方向認証）され、かつ親機１２－１が移動端末装置１１－１の本親機である場合のみ、リソースを要求し、利用することができる。

【０１６６】

これにより、移動端末装置１１－１と親機１２－１の両者間での通信中のデータ秘匿が可能となる。

【０１６７】

ステップＳ６２において、CPU１１１は、移動端末装置１１－１からリソース要求信号が供給されたと判定した場合、ステップＳ７３に進み、リソース送信処理を行い、その後、処理を終了する。リソース送信処理の詳細は、図９と図１０で後述する。

【０１６８】

一方、ステップＳ７２において、CPU１１１は、リソース要求信号が供給されていないと判定した場合、ステップＳ６２に戻り、上述した処理を繰り返す。

【０１６９】

図９は、移動端末装置１１－１および１１－２と直接無線通信が可能な親機１２－１が図８のステップＳ７３の処理で行うリソース送信処理を説明するフローチャートである。

【０１７０】

ステップＳ８１において、親機１２－１のCPU１１１は、図８のステップＳ７２で受信したリソース要求信号が自身が本親機となる移動端末装置（移動端末装置１１－１）からのリソース要求信号であるかどうかを判定する。ステップＳ８１において、親機１２－１のCPU１１１は、受信したリソース要求信号が自身が本親機となる移動端末装置１１－１からのリソース要求信号であると判定した場合、ステップＳ８２をスキップしてステップＳ８３に進む。

【０１７１】

ステップＳ８３では、親機１２－１のCPU１１１は、入出力部１１４を制御し、移動端末装置１１－１からのリソース要求信号に基づいて、移動端末装置１１

－１から要求されているリソースを有するリソース機器１５からリソースを取得し、ステップＳ８４に進む。ステップＳ８４では、親機１２－１のCPU１１１は、そのリソースを、移動端末装置１１－１に送信してリターンする。

【０１７２】

即ち、親機１２－１は、個人情報を格納しているユーザが使用する移動端末装置１１－１から、親機１２－１の接続するリソース機器１５の有するリソースを要求された場合、無条件に利用を許可する。

【０１７３】

一方、ステップＳ８１において、親機１２－１のCPU１１１は、図８のステップＳ７２で受信したリソース要求信号が、自身が本親機とならない移動端末装置からのリソース要求信号である（移動端末装置１１－２からのリソース要求信号である）と判定した場合、ステップＳ８２に進み、権利文の提示がある（リソース要求信号とともに権利文が送信されてきた）かどうかを判定する。ステップＳ８２において、親機１２－１のCPU１１１は、権利文の提示がなかったと判定した場合、移動端末装置１１－２はリソースを利用する権利がないので、処理を終了する。

【０１７４】

ステップＳ８２において、親機１２－１のCPU１１１は、権利文の提示があったと判定した場合、ステップＳ８３に進み、入出力部１１４を制御し、移動端末装置１１－２からのリソース要求信号に基づいて、移動端末装置１１－２から要求されているリソースを有するリソース機器１５からリソースを取得し、ステップＳ８４に進む。ステップＳ８４では、親機１２－１のCPU１１１は、そのリソースを、移動端末装置１１－２に送信する。

【０１７５】

即ち、親機１２－１は、個人情報を格納していないユーザが使用する移動端末装置１１－２から、親機１２－１に接続しているリソース機器１５の有するリソースを要求された場合、移動端末装置１１－２がリソースを利用する権利文を取得している場合のみ、リソース利用を許可する。逆に言えば、移動端末装置１１－２のユーザは、本親機１２－１のリソースを、そのリソースを利用する権利文

を、親機１２－１に提示したときのみ利用することができる。

【０１７６】

なお、親機１２－１は、親機１２－２が移動端末装置１１－２のユーザを認証するときのやりとり時に、移動端末装置１１－２は、そのユーザの個人情報を、その本親機である親機１２－２から取得する。ここで、個人情報には、そのユーザがリソースを利用したときの操作履歴などが含まれる。即ち、移動端末装置１１－２の本親機である親機１２－２は、例えば、そのユーザが自身の有するリソースを利用したときに、その利用時の操作履歴などを個人情報として登録する個人情報管理機能を有する。移動端末装置１１－２は、親機１２－１のリソースを利用するときに、ユーザの個人情報に応じて、移動端末装置１１－２のユーザの嗜好に合わせた操作性（ユーザＩ／Ｆ）を提供する。

【０１７７】

図１０は、移動端末装置１１－２がその本親機である親機１２－２と直接無線通信できない場合に、その親機１２－２が図８のステップＳ７１の処理で行うリソース送信処理を説明するフローチャートである。なお、親機１２－２は、認証装置１３から発行された電子証明書（図１１で後述する）を既に受信し、RAM１１３に保持しているものとする。

【０１７８】

ステップＳ１００において、親機１２－２のCPU１１１は、暗号化した利用権発行要求文と、RAM１１３に保持している電子証明書を作成し、その利用権発行要求文と電子証明書を、移動端末装置１１－１がリソースを利用しようとする本親機でない親機１２－１に送信する。即ち、親機１２－２のCPU１１１は、直接無線通信することができない移動端末装置１１－２から送信されたリソース要求信号に基づいて、リソース情報の識別子と利用方法を明記した利用権発行要求文を作成する。

【０１７９】

また、親機１２－２のCPU１１１は、リーダライタ１１５を制御し、非接触ＩＣカード１２１から読み込んだ秘密鍵３８をRAM１１３に保持する。CPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した秘密鍵３８を用いて、電子

署名を暗号化し、利用権発行要求文を付加する。そして、CPU１１１は、その利用権発行要求文を電子証明書とともに、移動端末装置１１－２がリソースを利用しようとしている親機１２－１に送信する。

【０１８０】

なお、利用権発行要求文とは、ここでは、移動端末装置１１－２が、その本親機でない親機１２－１のリソースの利用をするための利用権の発行を、親機１２－１に要求するメッセージである。

【０１８１】

また、移動端末装置１１－２が本親機である親機１２－２に送信するリソース要求信号には、その移動端末装置１１－２がリソースを利用しようとする本親機でない親機１２－２へアクセスするためのアクセス情報が含まれている。そして、親機１２－２は、このアクセス情報に基づいて、利用権発行要求文を親機１２－１に送信する。

【０１８２】

ステップＳ１００の処理後は、ステップＳ１０１に進み、親機１２－２のCPU１１１は、後述する図１３のステップＳ１４７で、利用権はおっ光要求文を受信した親機１２－１が親機１２－２に対して送信するリソースの利用を許可するための対価（バリュー）と対価の送信先口座情報を記載したリソース利用条件文と電子証明書を受信したかどうかを判定する。ステップＳ１０１において、親機１２－２のCPU１１１は、リソース利用条件文と電子証明書を受信したと判定した場合、暗号/復号部１１７を制御し、電子証明書に含まれる、親機１２－１の秘密鍵３５に対応する公開鍵３９を用いて、リソース利用条件文に含まれる電子署名を復号し、ステップＳ１０１からステップＳ１０２に進む。

【０１８３】

ステップＳ１０２において、親機１２－２のCPU１１１は、リソース利用条件文が正当であるかどうかを判定する。即ち、CPU１１１は、リソース利用条件文に含まれる電子署名が正常に復号されたかどうかを判定する。ステップＳ１０２において、CPU１１１は、リソース利用条件文が正当ではないと判定した場合、親機１２－１の秘密鍵３５で暗号化された電子署名が、それと対の公開鍵３９で

復号できていないので、親機１２－１と親機１２－２が通信する間で改ざんが行われたと判定し、処理を終了する。

【０１８４】

また、ステップＳ１０２において、親機１２－２のCPU１１１は、リソース利用条件文が正当であると判定した場合、秘密鍵３５で暗号化された電子署名が、公開鍵３９で復号できるので、親機１２－１と親機１２－２が通信する間で改ざんが行われず、親機１２－１と親機１２－２が正当な関係であると認識し、ステップＳ１０２からステップＳ１０３に進む。

【０１８５】

このように、電子署名を用いてリソース利用条件文が正当であるかどうかを判定することにより、通信システム１の安全性をさらに高めることができる。

【０１８６】

ステップＳ１０３において、親機１２－２のCPU１１１は、リソース利用条件文に基づいて、親機１２－２から親機１２－１にバリューを移動する（対価を支払う）ためのバリュー移動要求をバリュー発行装置１４に送信する。

【０１８７】

ステップＳ１０３の処理後は、ステップＳ１０４に進み、親機１２－２のCPU１１１は、バリュー発行装置１４から、後述する図１６のステップＳ１６２で送信される暗号化された共通秘密鍵４４を受信したかどうかを判定する。ステップＳ１０４において、CPU１１１は、バリュー発行装置１４から暗号化された共通秘密鍵４４を受信していないと判定した場合、バリュー発行装置１４から暗号化された共通秘密鍵４４が受信されるまで待機する。

【０１８８】

ステップＳ１０４において、親機１２－２のCPU１１１は、バリュー発行装置１４から暗号化された共通秘密鍵４４を受信したと判定した場合、ステップＳ１０５に進み、親機１２－２のCPU１１１は、バリュー発行装置１４の有する秘密鍵４３に対応する公開鍵４１を、認証装置１３から取得し、RAM１１３に保持する。そして、親機１２－２のCPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した公開鍵４１を用いて、暗号化された共通秘密鍵４４を復号し、復

号した共通秘密鍵４４をRAM１１３に保持する。

【０１８９】

ステップＳ１０５の処理後は、ステップＳ１０６に進み、親機１２－２のCPU１１１は、リーダライタ１１５を制御して、共通秘密鍵３７を読み込み、RAM１１３に保持し、ステップＳ１０７に進む。ステップＳ１０７では、親機１２－２のCPU１１１は、RAM１１３から復号した共通秘密鍵４４と共通秘密鍵３７を読み出し、両者が等しいかどうかを判定する。

【０１９０】

ステップＳ１０７において、親機１２－２のCPU１１１は、復号した共通秘密鍵４４と共通秘密鍵３７が等しいと判定した場合、即ち、後述する図１６のステップS１６１でバリュー発行装置１４により秘密鍵４３を用いて暗号化された共通秘密鍵４４が、ステップＳ１０６で親機１２－２により公開鍵４１を用いて正常に復号され、共通秘密鍵３７と等しい共通秘密鍵４４が得られている場合、親機１２－２のCPU１１１は、バリュー発行装置１４と親機１２－２が通信する間で改ざんがなかったことが認識し、ステップＳ１０７からステップＳ１０８に進む。

【０１９１】

従って、CPU１１１は、Ｓ１０８では、親機１２－２のCPU１１１は、暗号/復号部１１７を制御し、RAM１１３に保持した公開鍵４１を用いて、RAM１１３に保持した共通秘密鍵３７を暗号化する。ステップＳ１０９の処理後は、ステップＳ１１０に進み、親機１２－２のCPU１１１は、その暗号化した共通秘密鍵３７を、バリュー発行装置１４に送信し、リターンする。

【０１９２】

一方、ステップＳ１０７において、親機１２－２のＣＰＵ１１１は、ステップＳ１０６で復号した共通秘密鍵と共通秘密鍵３４が等しくないと判定した場合、バリュー発行装置１４と親機１２－２が通信する間で改ざんがあったと認識し、ステップＳ１１０に進み、バリュー発行装置１４に、バリュー発行装置１４と親機１２－２の関係は正当ではないことを示すエラーを通知してリターンする。

【０１９３】

また、ステップＳ１０１において、親機１２－２のCPU１１１は、移動端末装置１２－２がリソースを利用しようとする親機１２－１からのリソース利用条件文を受信していないと判定した場合、ステップＳ１１１に進み、親機１２－１から、後述する図１３のステップＳ１４８で送信されたるリソース利用条件文を発行できないことを示すエラー通知を受信したかどうかを判定する。ステップＳ１１０において、親機１２－２のCPU１１１は、親機１２－１からエラー通知を受信していないと判定した場合、ステップＳ１０１に戻り、上述した処理を繰り返す。

【０１９４】

また、ステップＳ１１１において、親機１２－２のCPU１１１は、親機１２－１からエラー通知を受信したと判定した場合、即ち、親機１２－１がリソース利用条件文を発行せず、移動端末装置１１－２によるリース利用を許可しなかった場合、処理を終了する。

【０１９５】

図１１は、電子証明書の例を示す図である。

【０１９６】

この電子証明書は、図１１に示されるように、証明書のバージョン番号、証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証装置１３の名前、証明書の有効期限、発行された装置のＩＤ、および装置の公開鍵が含まれている。

【０１９７】

この電子証明書は、認証装置１３により、親機１２－１、親機１２－２、およびバリュー発行装置１４に対して発行される。親機１２－１、親機１２－２、およびバリュー発行装置１４は、自らの正当性を証明するために他の装置に、暗号文とともにこの電子証明書を送信する。受信した装置は、この電子証明書に含まれる装置の公開鍵を用いて、この電子証明書とともに送信されてくる暗号文を復号し、その暗号文の正当性を認識することができる。

【０１９８】

図１２は、図６の親機１２－１がリソース情報を送信する処理を説明するフロ

ーチャートである。この処理は、例えば、親機１２－１が図５のステップＳ４１で移動端末装置１１－２から送信されるブロードキャスト要求信号を受信したとき開始される。

【０１９９】

ステップＳ１２０において、親機１２－１のCPU９１は、移動端末装置１１－２によるブロードキャスト要求を許可するかどうかを判定する。ステップＳ１２０において、親機１２－１のCPU９１は、ブロードキャスト要求を許可すると判定した場合、ステップＳ１２１に進み、移動端末装置１１－２にブロードキャスト要求許可の通知を送信する。

【０２００】

ステップＳ１２１の処理後は、ステップＳ１２２に進み、親機１２－１のCPU９１は、移動端末装置１１－２から図５のステップＳ４３でリソース情報要求信号が送信されて来るのを待って受信し、ステップＳ１２３に進む。

【０２０１】

ステップＳ１２３において、親機１２－１のCPU９１は、入出力部９７を制御し、データバス９８とリソース制御部９９を介して、リソース機器１５－１とリソース機器１５－２から、移動端末装置１２－２に提供することができる、または提供してもよいリソースのリソース情報を取得する。同様に、CPU９１は、入出力部９７を制御し、データバス９８を介して、リソース機器１６－１とリソース機器１６－２からリソース情報を取得する。そして、CPU９１は、取得したリソース情報を移動端末装置１１－２に送信して処理を終了する。

【０２０２】

一方、ステップＳ１２０において、CPU９１は、移動端末装置１１－２からのブロードキャスト要求を許可しないと判定した場合、ステップＳ１２４に進み、移動端末装置１１にブロードキャスト要求を許可しないことを示すエラー通知を送信し、処理を終了する。

【０２０３】

図１３は、図６の親機１２－１が、リソース利用条件文を発行するときに行うリソース利用条件文発行処理を説明するフローチャートである。この処理は、親

機１２－１が図１０のステップＳ１００の処理で親機１２－２から送信された、暗号化された利用権発行要求文と電子証明書を受信したとき開始される。なお、親機１２－１は、認証装置１３から発行された電子証明書（図１１）を既に受信し、RAM１１３に保持しているものとする。

【０２０４】

ステップＳ１４１において、親機１２－１のCPU１１１は、親機１２－２から利用権発行要求文とともに受信した電子証明書から公開鍵４０を取得し、ステップＳ１４２に進む。ステップＳ１４２では、親機１２－１のCPU１１１は、親機１２－２から受信した利用権発行要求文から秘密鍵３８を用いて暗号化された電子署名を取得する。CPU１１１は、暗号/復号部１１７を制御して、電子署名を、ステップＳ１４１で取得した、秘密鍵３８と対の公開鍵４０を用いて復号する。

【０２０５】

ステップＳ１４２の処理後は、ステップＳ１４３に進み、親機１２－１のCPU１１１は、利用権発行要求文が正当であるかどうかを判定する。即ち、親機１２－１のCPU１１１は、ステップＳ１４２で電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵３８で暗号化された電子署名が、秘密鍵３８に対応する公開鍵４０で正常に復号されているので、親機１２－１と親機１２－２が通信する間で改ざんが行われていないと認識し、利用権発行要求文が正当であると判定する。

【０２０６】

ステップＳ１４３において、親機１２－１のCPU１１１は、利用権発行要求文が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップＳ１４８に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

【０２０７】

ステップＳ１４３において、親機１２－１のCPU１１１は、利用権発行要求文が正当であると判定した場合、ステップＳ１４４に進み、親機１２－２から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置１３に送信し、ステップＳ１４５に進む。

【０２０８】

ステップＳ１４５では、親機１２－１のCPU１１１は、認証装置１３から、図１８のステップＳ１８３またはステップＳ１８４で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

【０２０９】

ステップＳ１４５において、親機１２－１のCPU１１１は、認証装置１３から電子証明書の対価を受信したと判定した場合、ステップＳ１４６に進み、その認証装置１３からの電子証明書の評価が有効であるかどうかを判定する。ステップＳ１４６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したと判定した場合、即ち、利用件発行要求とともに送信されてきた電子証明書が失効していない（無効でない）場合、ステップＳ１４７に進み、リソース利用を許可するための対価を記載したリソース利用条件文を電子的に作成する。

【０２１０】

このとき、親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、自らの正当性を証明するために、秘密鍵３５を用いて電子署名を暗号化し、リソース利用条件文に電子署名を付加する。そして、CPU１１１は、電子署名を付加した利用条件文と、RAM１１３に保持した電子証明書を、親機１２－２に送信し、処理を終了する。

【０２１１】

一方、ステップＳ１４６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップＳ１４８に進み、リソース利用の不許可を示すエラー通知を親機１２－２に送信し、処理を終了する。

【０２１２】

なお、親機１２－１がリソースを利用する権利を記載した権利文を発行する処理も、図１３と同様にして行われる。但し、この権利文を発行する処理は、バリ

ュー発行装置１４から、後述する図１６のステップＳ１６８で送信される暗号化された振込み通知書と電子証明書を受信したとき開始される。

【０２１３】

即ち、図１４は、図６の親機１２－１がリソースを利用するための権利文を発行するときに行う権利文発行処理を説明するフローチャートである。この処理は、親機１２－１が後述する図１６のステップＳ１６８の処理でバリュー発行装置１４から送信される、振込み通知書と電子証明書を受信したとき開始される。なお、親機１２－１は、認証装置１３から発行された電子証明書（図１１）を既に受信し、RAM１１３に保持しているものとする。

【０２１４】

ステップＳ１５１において、親機１２－１のCPU１１１は、バリュー発行装置１４から、振り込み通知書とともに受信した電子証明書から公開鍵４１を取得し、ステップＳ１５２に進む。ステップＳ１５２では、親機１２－１のCPU１１１は、バリュー発行装置１４から受信した振込み通知書から秘密鍵４３を用いて暗号化された電子署名を取得する。親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、電子署名を、ステップＳ１５１で取得した公開鍵４１を用いて復号する。

【０２１５】

ステップＳ１５２の処理後は、ステップＳ１５３に進み、親機１２－１のCPU１１１は、振込み通知書が正当であるかどうかを判定する。即ち、CPU１１１は、電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵４３で暗号化された電子署名が、秘密鍵４３に対応する公開鍵４１で正常に復号されているので、親機１２－１とバリュー発行装置１４が通信する間で改ざんが行われていないと認識し、振込み通知書が正当であると判定する。

【０２１６】

ステップＳ１５３において、親機１２－１のCPU１１１は、振込み通知書が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップＳ１５８に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

【０２１７】

また、ステップＳ１５３において、親機１２－１のCPU１１１は、振込み通知書が正当であると判定した場合、ステップＳ１５４に進み、バリュー発行装置１４から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置１３に送信し、ステップＳ１５５に進む。

【０２１８】

ステップＳ１５５では、親機１２－１のCPU１１１は、認証装置１３から、後述する図１８のステップＳ１８３またはステップＳ１８４で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

【０２１９】

そして、ステップＳ１５５において、親機１２－１のCPU１１１は、認証装置１３から電子証明書の評価を受信したと判定した場合、ステップＳ１５６に進み、CPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したかどうかを判定する。ステップＳ１５６において、CPU１１１は、認証装置１３から電子証明書は有効であるという評価を受信したと判定した場合、ステップＳ１５７に進み、リソースを利用する権利を記載した権利文を電子的に作成する。このとき、親機１２－１のCPU１１１は、暗号/復号部１１７を制御して、自らの正当性を証明するために、秘密鍵３５を用いて電子署名を暗号化し、権利文に電子署名を付加する。そして、親機１２－１のCPU１１１は、電子署名を付加した権利文と、RAM１１３に保持した電子証明書を、親機１２－２に送信して処理を終了する。

【０２２０】

一方、ステップＳ１５６において、親機１２－１のCPU１１１は、認証装置１３から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップＳ１５８に進み、リソース利用の不許可を示すエラー通知を親機１２－２に送信して処理を終了する。

【０２２１】

図１５は、図１のバリュー発行装置１４の詳細構成例である。

【０２２２】

バリュー発行装置１４は、通信部１３１、データバス１３２、共通秘密鍵認証部１３３、公開鍵認証部１３４、バリュー発行部１３５、共通秘密鍵記憶部１３６、秘密鍵記憶部１３７、証明書記憶部１３８、発行履歴記憶部１３９、およびバリュー記憶部１４０から構成されている。

【０２２３】

通信部１３１は、インターネット２１を介して、親機１２－１、親機１２－２、および認証装置１３からの信号を受信するとともに、親機１２－１、親機１２－２、および認証装置１３に信号を送信する。通信部１３１は、データバス１３２を介して、共通秘密鍵認証部１３３、公開鍵認証部１３４、およびバリュー発行部１３５に接続されている。

【０２２４】

共通秘密鍵認証部１３３は、共通秘密鍵記憶部１３６に記憶された共通秘密鍵４４に基づいて、バリュー発行装置１４にアクセスしてきた親機１２が正当であるかどうかを判定する。また、共通秘密鍵認証部１３３は、バリュー発行装置１４がバリューを管理する親機１２に対して、共通秘密鍵４４と同一の秘密鍵３４または３７を送信し、親機１２の非接触ＩＣカード１２１に記憶させる。

【０２２５】

このように、親機１２の非接触ＩＣカード１２１にバリュー発行装置１４の共通秘密鍵４４と等しい共通秘密鍵３４または３７を記憶させることにより、親機１２とバリュー発行装置１４との間での認証が可能となり、ユーザが、その親機１２と通信が可能な移動端末装置１１を使用するだけで、バリュー発行装置１４を介して、親機１２どうしの間でのバリューの移動をすることができる。

【０２２６】

公開鍵認証部１３４は、秘密鍵記憶部１３７に記憶された秘密鍵４３や、証明書記憶部１３８に記憶された電子証明書を用いて、親機１２－１、親機１２－２、および認証装置１３との間で通信部１３１を開始、公開鍵暗号系の処理を行なう。

【０２２７】

バリュー発行部１３５は、バリュー記憶部１４０に記憶されたバリュー（電子バリュー）に基づき、バリューを発行し、その発行履歴を発行履歴記憶部１３９に記憶させる。

【０２２８】

なお、バリュー発行装置１４は、物理的に１つの筐体に入る必要はなく、データバス１３２を経由して複数の機器が協調して機能を実現してもよい。

【０２２９】

また、バリュー発行装置１４は、発行したバリューに応じた対価を決済できるようにしてもよい。さらに、親機１２は、所有する電子バリューをネットワークでの決済に使用してもよい。

【０２３０】

また、電子バリューの形式は何でもよい。電子バリューはバリュー発行装置１４のバリュー記憶部１４０に口座という形で格納してもよい。この場合、より高い安全性を提供することができる。

【０２３１】

さらに、バリューは、バリュー発行装置１４のバリュー記憶部１４０に口座という形で記憶されるだけでなく、親機１２の安全なデバイス（例えば、非接触ＩＣカード１２１）の記憶領域へ格納されてもよい。この場合、バリュー発行装置１４のバリュー発行部１３５で発行された電子バリューは、親機１２の非接触ＩＣカード１２１に転送される。例えば、バリュー発行装置１４が、親機１２－２から親機１２－１に対してバリューを振り込む場合、バリュー発行装置１４は、親機１２－２からバリューを取得し、バリューを親機１２－１に送信する。なお、バリューの送受信は、バリューを暗号化して安全に行われる。

【０２３２】

また、バリューは、バリュー発行装置１４のバリュー記憶部１４０および親機１２の安全なデバイスの両者の組み合わせによって記憶されてもよい。この組み合わせとして、バリュー発行装置１４は、ユーザの電子バリューをバリュー記憶部１４０の中でそれぞれのユーザの口座として記憶し、その口座を管理しつつ、

必要な額だけをユーザのデバイス（例えば、非接触ＩＣカード）へ移動させ財布のように利用させてもよい。

【０２３３】

図１６は、図１５のバリュー発行装置１４が振り込み通知書を親機１２－１に送信する処理を説明するフローチャートである。この処理は、バリュー発行装置１４が、親機１２－２が図１０のステップＳ１０３で送信したバリュー移動要求を受信したとき開始される。なお、バリュー発行装置１４は、認証装置１３が発行した電子証明書を、既に証明書記憶部１３８に記憶しているものとする。

【０２３４】

ステップＳ１６１において、共通秘密鍵認証部１３３は、共通秘密鍵記憶部１３６から共通秘密鍵４４と、秘密鍵記憶部１３７から秘密鍵４３を読み出し、秘密鍵４３を用いて、共通秘密鍵４４を暗号化する。ステップＳ１６１の処理後は、ステップＳ１６２に進み、共通秘密鍵認証部１３３は、その暗号化された共通秘密鍵４４を親機１２－２に送信し、ステップＳ１６３に進む。即ち、共通秘密鍵認証部１３３は、暗号化された共通秘密鍵４４を、データバス１３２を介して通信部１３１に供給し、通信部１３１は、その暗号化された共通秘密鍵４４を親機１２－２に送信する。

【０２３５】

ステップＳ１６３において、通信部１３１は、親機１２－２から、図１０のステップＳ１０９で送信された暗号化された共通秘密鍵３７を受信したかどうかを判定する。ステップＳ１６３において、通信部１３１は、親機１２－２から暗号化された共通秘密鍵３７を受信していないと判定した場合、ステップＳ１６４に進み、親機１２－２から、図１０のステップＳ１１０で送信される、バリュー発行装置１４と親機１２－２の関係が正当ではないことを示すエラー通知を受信したかどうかを判定する。ステップＳ１６８において、通信部１３１は、エラー通知を受信していないと判定した場合、ステップＳ１６３に戻り、上述した処理を繰り返す。

【０２３６】

ステップＳ１６４において、通信部１３１は、エラー通知を受信したと判定し

た場合、バリュー発行装置１４と親機１２－２の関係が正当ではないので、バリュー移動の不許可を示すエラー通知を送信して処理を終了する。

【０２３７】

一方、ステップＳ１６３において、通信部１３１は、親機１２－２から暗号化された共通秘密鍵３７を受信したと判定した場合、その暗号化された共通秘密鍵３７を公開鍵認証部１３４に供給し、ステップＳ１６３からステップＳ１６５に進む。ステップＳ１６５において、公開鍵認証部１３４は、暗号化された共通秘密鍵３７を、秘密鍵記憶部１３７に記憶している秘密鍵４３を用いて復号する。

【０２３８】

ステップＳ１６５の処理後は、ステップＳ１６６に進み、公開鍵認証部１３４は、共通秘密鍵認証部１３３に、ステップＳ１６５で復号した共通秘密鍵３７を供給し、共通秘密鍵認証部１３３は、復号した共通秘密鍵３７と共通秘密鍵記憶部１３６に記憶している共通秘密鍵４４が等しいかどうかを判定する。

【０２３９】

ステップＳ１６６において、共通秘密鍵認証部１３３は、復号した共通秘密鍵３７と共通秘密鍵４４が等しいと判定した場合、親機１２－２とバリュー発行装置１４の関係は正当であると認識して、ステップＳ１６６からステップＳ１６７に進む。即ち、この場合、親機１２－１において公開鍵４１を用いて暗号化された共通秘密鍵３７が、バリュー発行装置１４において、公開鍵４１に対応する秘密鍵４３を用いて正常に復号され、共通秘密鍵３７が得られているので、バリュー発行装置１４は、親機１２－２とバリュー発行装置１４が通信する間で改ざんが行われていないと認識する。

【０２４０】

さらに、バリュー発行装置１４は、親機１２－２が有する共通秘密鍵３７とバリュー発行装置１４が有する共通秘密鍵４４が等しいので、親機１２－２がバリューを管理することを認められている相手であることを認識する。即ち、バリュー発行装置１４は、バリュー発行装置１４の有する共通秘密鍵４４と同一の秘密鍵３７を、親機１２－２に備えられる安全なデバイス（非接触ＩＣカード１２１）に配布し、親機１２－２が共通秘密鍵４４と等しい共通秘密鍵３７を有するこ

とを認識することによって、正しい親機１２－２からのアクセスであることを認識する。

【０２４１】

ステップＳ１６７において、バリュー発行部１３５は、親機１２－２から親機１２－１にバリューを移動する。即ち、バリュー発行部１３５は、バリュー記憶部１４０に記憶された親機１２－２の所定の対価に対応するバリューを削除し、親機１２－１のバリューに所定の対価に対応するバリューを追加し、これにより、親機１２－２のユーザの電子バリューが、そのユーザが移動端末装置１１－２によってリソースを利用しようとしている親機１２－１のユーザに対し、そのリソースの利用に対する対価として振り込まれる。さらに、ステップＳ１６７では、バリュー発行部１３５は、バリューの移動完了を示す取引結果通知を生成する。

【０２４２】

これにより、ユーザは、バリュー発行装置１４を経由して、他のユーザとの間で、電子バリューの授受を行うことができる。

【０２４３】

ステップＳ１６７の処理後は、ステップＳ１６８に進み、公開鍵認証部１３４は、秘密鍵記憶部１３７に記憶された秘密鍵４３を用いて、自らの正当性を証明するために電子署名を暗号化する。そして、公開鍵認証部１３４は、その暗号化した電子署名を付加した振込み通知書を作成する。この振込み通知書は、バリューの振込みを知らせるための振込み通知と、バリューの振込みの詳細が記載されたレシートから構成されている。そして、公開鍵認証部１３４は、その振込み通知書、証明書記憶部１３８に記憶された電子証明書、および電子バリューの移動完了を示す取引結果通知を、バリューの振込先であるユーザの親機１２－１に送信して処理を終了する。

【０２４４】

一方、ステップＳ１６６において、共通秘密鍵認証部１３３は、ステップＳ１６５で復号した共通秘密鍵と共通秘密鍵４４が等しくないと判定した場合、親機１２－２とバリュー発行装置１４の関係は正当ではないので、バリュー移動の不

許可を示すエラー通知を送信して処理を終了する。

【０２４５】

図１７は、図１の認証装置１３の詳細構成例を示している。

【０２４６】

認証装置１３は、通信部１５１、データバス１５２、公開鍵認証部１５３、秘密鍵記憶部１５４、証明書記憶部１５５、公開鍵記憶部１５６、証明書記憶部１５７、および証明書失効リスト記憶部１５８から構成されている。

【０２４７】

通信部１５１は、インターネット２１を介して、親機１２－１、親機１２－２、およびバリュー発行装置１４から送信された信号を受信するとともに、親機１２－１、親機１２－２、およびバリュー発行装置１４に信号を送信する。通信部１５１は、データバス１５２を介して、公開鍵認証部１５３と接続されている。

【０２４８】

公開鍵認証部１５３は、公開鍵記憶部１５６に記憶された公開鍵と、一般公開用証明書記憶部１５７に記憶された一般公開用証明書を公開したり、電子証明書を発行する。また、公開鍵認証部１５３は、電子証明書が有効であるかどうかを判定する。

【０２４９】

秘密鍵記憶部１５４には、秘密鍵４２が記憶される。証明書記憶部１５５には、認証装置１３の電子証明書が記憶される。公開鍵記憶部１５６には、親機１２－１の秘密鍵３５に対応する公開鍵３９、親機１２－２の秘密鍵３８に対応する公開鍵４０、およびバリュー発行装置１４の秘密鍵４３に対応する公開鍵４１が記憶される。

【０２５０】

一般公開用証明書記憶部１５７には、公開鍵認証部１５３が発行した一般公開用の電子証明書が記憶され、この電子証明書が親機１２やバリュー発行装置１４に提供される。証明書失効リスト記憶部１５８には、失効した電子証明書を示す証明書失効リストが記憶される。即ち、一般公開用証明書記憶部１５７に記憶された電子証明書が何らかの理由により失効したとき、その電子証明書が、その証

明書失効リストにエントリされる。

【０２５１】

図１８は、図１７の認証装置１３が電子証明書の判定を行う処理を説明するフローチャートである。この処理は、親機１２などから電子証明書の有効性の判定を要求する信号を受信したとき開始する。

【０２５２】

ステップＳ１８１において、公開鍵認証部１５３は、証明書失効リスト記憶部１５８から、失効した電子証明書を示す証明書失効リストを読み出し、ステップＳ１８２に進む。ステップＳ１８２において、公開鍵認証部１５３は、親機１２から受信した電子証明書の判定を要求する信号に基づいて、判定の対象となる電子証明書が失効しているかどうかを判定する。即ち、公開鍵認証部１５３は、ステップＳ１８１で読み出された証明書失効リストに、判定の対象となる電子証明書があるかどうかを判定する。

【０２５３】

ステップＳ１８２において、公開鍵認証部１５３は、判定の対象となる電子証明書が失効していると判定した場合、ステップＳ１８３に進み、データバス１５２を介して通信部１５１から、親機１２に電子証明書の無効通知を送信して処理を終了する。

【０２５４】

ステップＳ１８２において、公開鍵認証部１５３は、判定の対象となる電子証明書が失効していないと判定した場合、ステップＳ１８４に進み、データバス１５２を介して通信部１５１から、親機１２に電子証明書の有効通知を送信して処理を終了する。

【０２５５】

図１９は、図１の通信システム１の全体の処理を説明するフローチャートである。即ち、図１９のフローチャートは、移動端末装置１１－１と移動端末装置１１－２が親機１２－１とのみ直接無線通信することができる場合に、その親機１２－１に接続されたリソース機器１５－１を利用するときの通信システム全体の処理を示している。

【０２５６】

なお、図１９では、移動端末装置１１－１、移動端末装置１１－２、親機１２－１、親機１２－１、認証装置１３、およびバリュー発行装置１４は、それぞれが通信する間で改ざんが行われず、正当な関係であるとする。

【０２５７】

また、図１９では、まず最初に、移動端末装置１１－１がその本親機である親機１２－１にリソースを要求し、その後、移動端末装置１１－２が、無線通信できるが本親機でない親機１２－１にリソースを要求するものとする。

【０２５８】

ステップＳ２３１において、移動端末装置１１－１は、その本親機である親機１２－１と双方向認証するために、共通秘密鍵３１を暗号化して、親機１２－１に送信する。

【０２５９】

ステップＳ２５１において、親機１２－１は、移動端末装置１１－１から暗号化された共通秘密鍵３１を受信する。ステップＳ２５２において、親機１２－１は、共通秘密鍵３３を暗号化し、移動端末装置１１－１に送信する。

【０２６０】

ステップＳ２３２において、移動端末装置１１－１は、親機１２－１から暗号化された共通秘密鍵３３を受信する。ステップＳ２３３において、移動端末装置１１－１は、その暗号化された共通秘密鍵３３を復号し、復号した共通秘密鍵３３を暗号化して、暗号化した共通秘密鍵３３を親機１２－１に送信する。

【０２６１】

ステップＳ２５３において、親機１２－１は、暗号化された共通秘密鍵３３を、移動端末装置１１－１から受信する。ステップＳ２５４において、親機１２－１は、暗号化された共通秘密鍵３３を復号する。親機１２－１は、復号した共通秘密鍵３３から、親機１２－１と移動端末装置１１－１の関係が正当であるかどうかを判定する。この例では、親機１２－１と移動端末装置１１－１は正当な関係であるので、親機１２－１は、ステップＳ２５１で移動端末装置１１－１から受信した暗号化された共通秘密鍵３１を復号し、その復号した共通秘密鍵３１を

暗号化して、移動端末装置１１－１に送信する。

【０２６２】

ステップＳ２３４において、移動端末装置１１－１は、親機１２－１から暗号化された共通秘密鍵３１を受信し、その暗号化された共通秘密鍵３１を復号する。移動端末装置１１－１は、復号した共通秘密鍵３１から、親機１２－１と移動端末装置１１－１の関係が正当であるかどうかを判定する。この例では、親機１２－１と移動端末装置１１－１の関係は正当であるので、双方向認証を完了し、ステップＳ２３５において、移動端末装置１１－１は、リソースを要求する信号を親機１２－１に送信する。

【０２６３】

即ち、移動端末装置１１－１は、その本親機である親機１２－１と双方向認証することにより、移動端末装置１１－１を使用するユーザが正しいユーザであることを、通信システム１のユーザに保証する。

【０２６４】

ステップＳ２５５において、親機１２－１は、移動端末装置１１－１からリソースを要求する信号を受信する。ステップＳ２５６において、親機１２－１は、リソースを要求する信号に基づいて、要求対象となるリソース機器１５－１にリソースを要求する信号を送信する。

【０２６５】

ステップＳ２９１において、リソース機器１５－１は、親機１２－１からリソースを要求する信号を受信する。ステップＳ２９２において、リソース機器１５－１は、リソースを要求する信号に基づいて、要求対象となるリソースを親機１２－１を介して、移動端末装置１１－１に送信する。

【０２６６】

ステップＳ２３６において、移動端末装置１１－１は、リソース機器１５－１から親機１２－１を介して、リソースを受信し、これにより、リソース機器１５－１を利用することが可能な状態となる。

【０２６７】

一方、移動端末装置１１－２は、ステップＳ２０１において、リソース情報を

取得するために、その本親機でない親機１２－１にブロードキャストを要求する信号を送信する。

【０２６８】

ステップＳ２５７において、親機１２－１は、移動端末装置１１－２からブロードキャストを要求する信号を受信し、ブロードキャスト要求を許可するかどうかを判定する。図１９では、ステップＳ２５８において、親機１２－１は、ブロードキャストを許可し、ブロードキャストを許可する信号を、移動端末装置１１－２に送信する。

【０２６９】

ステップＳ２０２において、移動端末装置１１－２は、親機１２－１からブロードキャストを許可する信号を受信する。ステップＳ２０３において、移動端末装置１１－２は、親機１２－１が取得できるリソースの情報（親機１２－１が、移動端末装置１１－２に提供することができるリソースの情報）を要求する信号を、親機１２－１に送信する。

【０２７０】

ステップＳ２５９において、親機１２－１は、移動端末装置１１－２からリソースの情報を要求する信号を受信する。ステップＳ２６０において、親機１２－１は、リソース情報を移動端末装置１１－２に送信する。

【０２７１】

ステップＳ２０４において、移動端末装置１１－２は、親機１２－１からリソース情報を受信する。ステップＳ２０５において、移動端末装置１１－２は、親機１２－２と双方向認証をするため、共通秘密鍵３２を暗号化し、その暗号化した共通秘密鍵３２を親機１２－２に送信する。

【０２７２】

ステップＳ３１１において、親機１２－２は、移動端末装置１１－２から、暗号化された共通秘密鍵３２を受信する。ステップＳ３１２において、親機１２－２は、共通秘密鍵３６を暗号化し、暗号化した共通秘密鍵３６を移動端末装置１２は、共通秘密鍵３６を暗号化し、暗号化した共通秘密鍵３６を移動端末装置１１-２に送信する。

【０２７３】

ステップＳ２０６において、移動端末装置１１-２は、親機１２-２から暗号化した共通秘密鍵３６を受信し、暗号化した共通秘密鍵３６を復号する。移動端末装置１１－２は、復号した共通秘密鍵３６から、移動端末装置１１－２と親機１２-２の関係が正当であるかどうかを判定する。この例の場合、移動端末装置１１－２と親機１２－２の関係は正当であるので、ステップＳ２０７において、移動端末装置１１－２は、復号した共通秘密鍵３６を暗号化し、暗号化した共通秘密鍵３６を親機１２-２に送信する。

【０２７４】

ステップＳ３１３において、親機１２－２は、移動端末装置１１－２から暗号化した共通秘密鍵３６を受信し、その暗号化した共通秘密鍵３６を復号する。親機１２－２は、復号した共通秘密鍵３６から、親機１２－２と移動端末装置１１-２の関係は正当であるかどうかを判定する。この例の場合、親機１２－２と移動端末装置１１－２の関係は正当であるので、ステップＳ３１４において、親機１２－２は、ステップＳ３１１で移動端末装置１１－２から受信した暗号化された共通秘密鍵３２を復号し、復号した共通秘密鍵３２を暗号化する。親機１２－２は、その暗号化した共通秘密鍵３２を移動端末装置１１－２に送信する。

【０２７５】

ステップＳ２０８において、移動端末装置１１－２は、親機１２－２から暗号化された共通秘密鍵３２を受信し、その暗号化された共通秘密鍵３２を復号する。移動端末装置１１－２は、復号した共通秘密鍵３２から、移動端末装置１１－２と親機１２－２の関係が正当であるかどうかを判定する。この例では、移動端末装置１１－２と親機１２－２の関係が正当であるので、双方向認証を完了し、ステップＳ２０９において、移動端末装置１１－２は、リソースを要求する信号を親機１２－２に送信する。

【０２７６】

ステップＳ３１５において、親機１２－２は、移動端末装置１１－２から、リソースを要求する信号を受信する。ステップＳ３１６において、親機１２－２は、親機１２－１にリソース情報の識別子と利用方法を明記した利用権発行要求と電子証明書を、親機１２－１に送信する。

【０２７７】

ステップＳ２６１において、親機１２－１は、親機１２－２から利用権発行要求と電子証明書を受信する。ステップＳ２６２において、親機１２－１は、その電子証明書が有効であるかどうかの判定要求を認証装置１３に送信する。

【０２７８】

ステップＳ３６１において、認証装置１３は、親機１２－１から電子証明書の判定要求を受信し、その電子証明書が有効であるかどうかを判定する。なお、ここでは、電子証明書は有効であるものとし、ステップＳ３６２において、認証装置１３は、親機１２－１に対象の電子証明書が有効であることを示す信号を送信する。

【０２７９】

ステップＳ２６３において、親機１２－１は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ２６４において、親機１２－１は、リソースの利用を許可するための対価を記載したリソース利用条件文と電子証明書を、親機１２－２に送信する。

【０２８０】

ステップＳ３１７において、親機１２－２は、親機１２－１からリソース利用条件文と電子証明書を受信する。ステップＳ３１８において、親機１２－２は、バリュー発行装置１４にバリュー移動要求を送信する。

【０２８１】

ステップＳ３４１において、バリュー発行装置１４は、親機１２－２からバリュー移動要求を受信する。ステップＳ３４２において、バリュー発行装置１４は、親機１２－２と双方向認証するため、共通秘密鍵４４を暗号化して、暗号化した共通秘密鍵４４を親機１２－２に送信する。

【０２８２】

ステップＳ３２０において、親機１２－２は、バリュー発行装置１４から、暗号化された共通秘密鍵４４を受信し、その暗号化された共通秘密鍵４４を復号する。親機１２－２は、復号した共通秘密鍵４４から、親機１２－２とバリュー発行装置１４の関係が正当であるかどうかを判定する。この例の場合、親機１２－

２とバリュー発行装置１４の関係は正当であるので、ステップＳ３２０において、親機１２－２は、共通秘密鍵３７を暗号化し、暗号化した共通秘密鍵３７をバリュー発行装置１４に送信する。

【０２８３】

ステップＳ３４３において、バリュー発行装置１４は、親機１２－２から暗号化された共通秘密鍵３７を受信し、その暗号化された共通秘密鍵３７を復号する。バリュー発行装置１４は、復号した共通秘密鍵３７から、バリュー発行装置１４と親機１２－２の関係が正当であるかどうかを判定する。この例の場合、バリュー発行装置１４と親機１２－２の関係は正当であるので、ステップＳ３４４において、バリュー発行装置１４は、ステップＳ３４１で受信したバリュー移動要求に応じてバリューを移動し、即ち、ここでは、親機１２－１のユーザから親機１２－１のユーザにバリューを移動し、バリューが移動されたことを示す振込み通知と電子証明書を、親機１２－１に送信する。

【０２８４】

ステップＳ２６５において、親機１２－１は、バリュー発行装置１４から、振込み通知書と電子証明書を受信する。ステップＳ２６６において、親機１２－１は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置１３に送信する。

【０２８５】

ステップＳ３６３において、認証装置１３は、親機１２－１から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機１２－２の電子証明書は有効であるので、ステップＳ３６４において、認証装置１３は、親機１２－１に対象の電子証明書が有効であることを示す信号を送信する。

【０２８６】

ステップＳ２６７において、親機１２－１は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ２６８において、親機１２－１は、リソースを利用する権利を記載した権利文を発行し、その権利文と電子証明書を親機１２－２に送信する。

【０２８７】

ステップＳ３２１において、親機１２－２は、親機１２－１から送信されてくる権利文と電子証明書を受信する。ステップＳ３２２において、親機１２－２は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置１３に送信する。

【０２８８】

ステップＳ３６５において、認証装置１３は、親機１２－２から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機１２－１の電子証明書は有効であるので、ステップＳ３６６において、認証装置１３は、親機１２－２に対象の電子証明書が有効であることを示す信号を送信する。

【０２８９】

ステップＳ３２３において、親機１２－２は、認証装置１３から電子証明書が有効であることを示す信号を受信する。ステップＳ３２４において、親機１２－２は、ステップＳ３２１で、親機１２－１から受信した権利文を、移動端末装置１１－２に送信する。

【０２９０】

ステップＳ２１０において、移動端末装置１１－２は、親機１２－１から権利文を受信する。ステップＳ２１１において、移動端末装置１１－２は、その権利文とリソースを要求する信号を、親機１２－１に送信する。

【０２９１】

ステップＳ２６９において、親機１２－１は、移動端末装置１１－２から、権利文とリソースを要求する信号を受信する。ステップＳ２７０において、親機１２－１は、リソース機器１５－１にリソースを要求する信号を送信する。

【０２９２】

ステップＳ２９３において、リソース機器１５－１は、親機１２－１からリソースを要求する信号を受信する。ステップＳ２９４において、リソース機器１５－１は、親機１２－１から要求されたリソースを親機１２－１を介して、移動端末装置１１－２に送信する。

【０２９３】

ステップＳ２１２において、リソース機器１５－１から、リソースを受信する。

【０２９４】

以上により、移動端末装置１１－２は、親機１２－１から権利文を取得することにより、親機１２－１に接続されたリソース機器１５－１を利用できる環境を得ることができる。

【０２９５】

以上のように、通信システム１では、バリュー発行装置１４は、バリューの管理をする親機１２に対して共通秘密鍵４４と同一の秘密鍵３４や３７を送信し、親機１２の非接触ＩＣカード１２１に記憶させる。親機１２は、個人情報を格納するユーザに、親機１２と通信可能にするための共通秘密鍵を格納した非接触ＩＣカード７１を発行する。これにより、ユーザは、非接触ＩＣカード７１の情報を移動端末装置１１に読み込ませるだけで、本親機である親機１２と通信をし、バリューの移動をすることができる。そして、ユーザは、上述した一連の処理を、例えば、非接触ＩＣカード７１を移動端末装置１１に、ワンタッチすることで行わせることができ、この場合、利便性の高い付加価値を提供することができる。

【０２９６】

さらに、認証情報やそれに伴うユーザの個人情報を管理する本親機となる親機１２を、例えばユーザ宅のホームサーバという形で、移動端末装置１１とは別に設けたので、ユーザと移動端末装置１１とは依存関係がなく、リソースの利用時にのみユーザの認証を行えば済む。また、ユーザは、個人情報をバリュー発行装置に管理させることなく、自らの所有する親機１２に格納し、バリューの決済情報だけを親機１２とバリュー発行装置１４との間でやりとりするだけで済む。さらに、ユーザが移動する場合においても、ユーザは、移動した空間にある機器（リソース）を、匿名のままユーザの嗜好に合わせた操作性で操作することができる。

【０２９７】

また、図１の通信システム１によれば、ユーザが、移動した空間にある移動端末装置１１－２を操作することにより、そのユーザが個人情報を管理する親機（本親機）１２－２が、バリュー発行装置１４の仲介の下、他人の親機１２－１に電子バリューを支払って、その親機１２－１のリソースの利用権を入手し、その利用権を、移動端末装置１１－２が受け取って、親機１２－１に提示することで移動端末装置１１－２のユーザは、他人の親機１２－１のリソースを、匿名のまま利用することができる。即ち、バリュー発行装置１４は、移動端末装置１１－２のユーザの親機１２－２から他人の親機１２－１に対しての電子バリューの振込みを仲介するだけであり、ユーザの個人情報の管理は、親機１２で行われる。従って、電子バリューの決済の場と、個人情報の管理の場とが完全に分離されているということができる。なお、移動端末装置１１－２からバリュー発行装置１４にアクセスし、電子バリューを、リソースを利用しようとする親機１２－１に振込み、移動端末装置１１－２から親機１２－１のリソースを利用することも可能である。但し、この場合、親機１２－１に対する、移動端末装置１１－２のユーザの匿名性は確保されるが、移動端末装置１１－２のユーザの個人情報の管理は、移動端末装置１１－２がアクセスするバリュー発行装置１４で行われることになる。

【０２９８】

さらに、移動端末装置１１－２は、リソースを利用する親機１２－１を介して、本親機である親機１２－２にアクセスして、そのリソースの利用権を取得するので、利用したいリソースに近い位置で、その利用権を得ることができる。

【０２９９】

ここで、移動端末装置１１としては、例えば、PDA(Personal Digital Assistant)や、携帯用コンピュータ、携帯電話機、腕時計、ディジタルスチルカメラ、デジタルビデオカメラなどの携帯性に優れた装置を採用することが可能である。

【０３００】

また、出先のユーザが移動端末装置１１から利用するリソースとしては、例えば、「装置」や、「情報」、「情報に対するライセンス」などがある。

【０３０１】

リソースとしての「装置」には、例えば、無線アクセスポイントや、テレビジョン受像機、電話機などが含まれる。リソースとして「装置」を利用するケースとしては、例えば、出先のユーザが、移動端末装置１１から、他人の無線アクセスポイントを利用してインターネットに接続する場合がある。

【０３０２】

また、リソースとしての「情報」には、いわゆるホームサーバやチャンネルサーバなどで構成される親機１２－１が管理するコンテンツその他の情報などが含まれる。リソースとして「情報」を利用するケースとしては、例えば、出先のユーザが、親機１２－１としてのチャンネルサーバに蓄えられたコンテンツを視聴する場合がある。

【０３０３】

さらに、リソースとしての「情報に対するライセンス」には、情報が暗号化されている場合に、その暗号化を解くための鍵などが含まれる。リソースとして「情報に対するライセンス」を利用するケースとしては、例えば、携帯端末装置１１に、ネットワーク経由でダウンロードした、暗号化されたコンテンツを視聴する場合に、そのコンテンツを視聴するためのライセンスとしての暗号鍵を取得するときなどがある。

【０３０４】

なお、上述した一連の処理では、移動端末装置１１－１と移動端末装置１１－２のユーザは異なっていたが、同一ユーザの親機や移動端末装置間でも同様に電子バリューの移動をすることができる。

【０３０５】

なお、本明細書において、フローチャートに記載された処理は、ステップとして記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０３０６】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

【０３０７】

【発明の効果】

以上の如く、本発明によれば、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作させることができる。また、そのとき発生する対価の支払いを自動的に行うことができる。さらに、利便性がよく、安全な通信をすることができる。

【図面の簡単な説明】

【図１】

本発明を適用した通信システムの構成例を示すブロック図である。

【図２】

図１の移動端末装置の構成例を示すブロック図である。

【図３】

図２の移動端末装置におけるリソース取得処理を説明するフローチャートである。

【図４】

図３のステップＳ２およびステップＳ６の共通秘密鍵認証処理を説明するフローチャートである。

【図５】

図３のステップＳ５のリソース情報取得処理を説明するフローチャートである。

【図６】

図１の親機の構成例を示す図である。

【図７】

図６のリソース制御部の構成例を示す図である。

【図８】

図６の親機におけるリソース制御処理を説明するフローチャートである。

【図９】

図８のステップＳ７１のリソース送信処理を説明するフローチャートである。

【図１０】

図８のステップＳ７１のリソース送信処理を説明するフローチャートである。

【図１１】

電子証明書の例を示す図である。

【図１２】

図６の親機におけるリソース情報送信処理を説明する図である。

【図１３】

図６の親機におけるリソース利用条件文発行処理を説明するフローチャートである。

【図１４】

図６の親機における権利文発行要求処理を説明するフローチャートである。

【図１５】

図１のバリュー発行装置の構成例を示す図である。

【図１６】

図１５のバリュー発行装置における振込み通知書送信処理を説明するフローチャートである。

【図１７】

図１の認証装置の構成例を示す図である。

【図１８】

図１７の認証装置における電子証明書判定処理を説明する図である。

【図１９】

図１の通信システムにおけるリソース取得処理を説明する図である。

【符号の説明】

１１　移動端末装置，　１２　親機，　１３　認証装置，　１４　バリュー発行装置，　１５　リソース，　１６　リソース，　２１　インターネット，　３１　共通秘密鍵，　３２　共通秘密鍵，　３３　共通秘密鍵，　３４　共通秘密鍵，　３５　秘密鍵，　３６　共通秘密鍵，　３７　共通秘密鍵，　３８　秘密鍵，　３９　公開鍵，　４０　公開鍵，　４１　公開鍵，　４２　秘密鍵，　４３　秘密鍵，　４４　共通秘密鍵，　６９　暗号/復号部　７１　非接触ＩＣカード，　１２１　非接触ＩＣカード，　１１７　暗号/復号部　１３３　共通秘

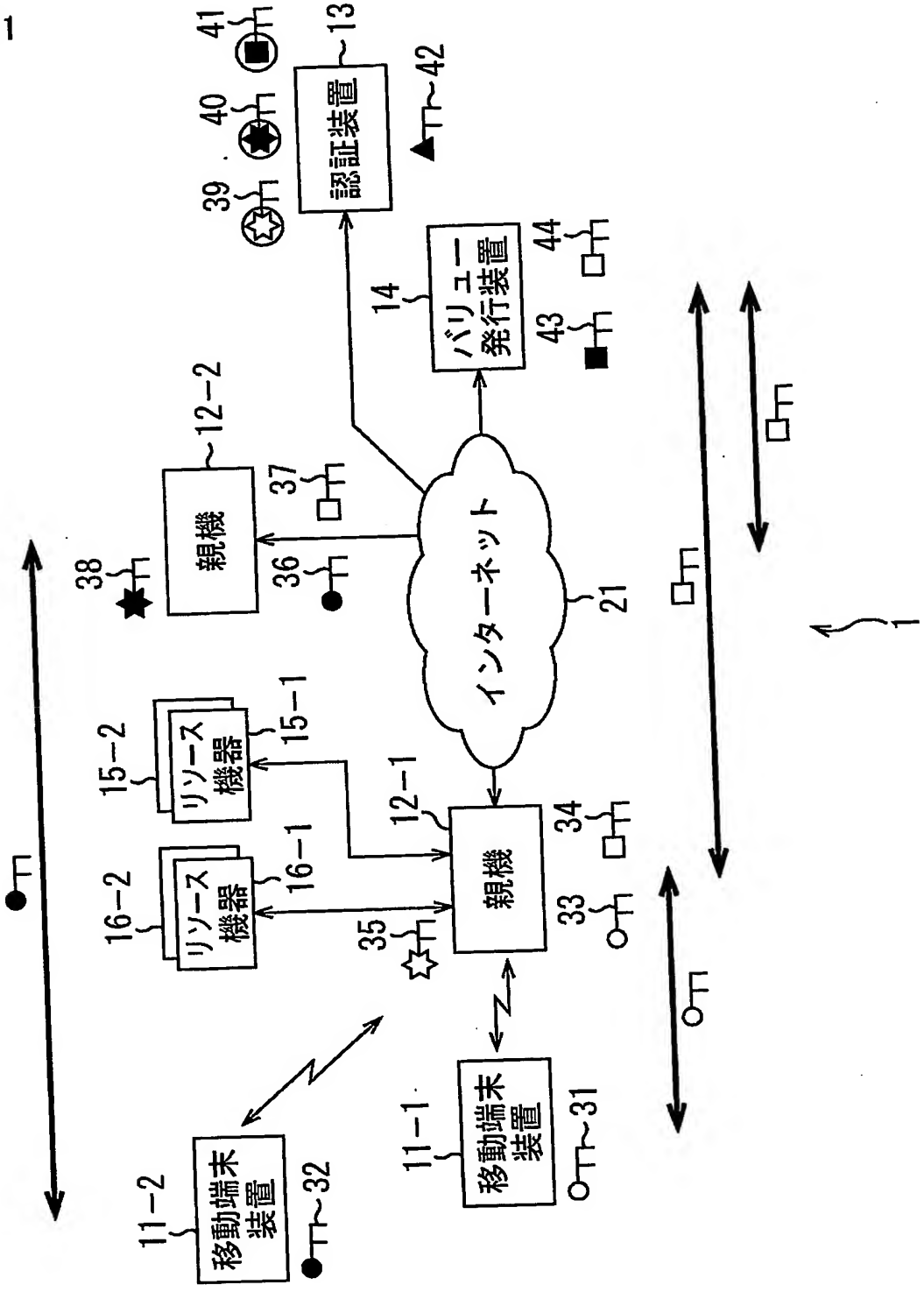
密鍵認証部，　１３４　公開鍵認証部，　１３５　バリュー発行部，　１５３

公開鍵認証部，　１５８　証明書失効リスト記憶部

【書類名】図面

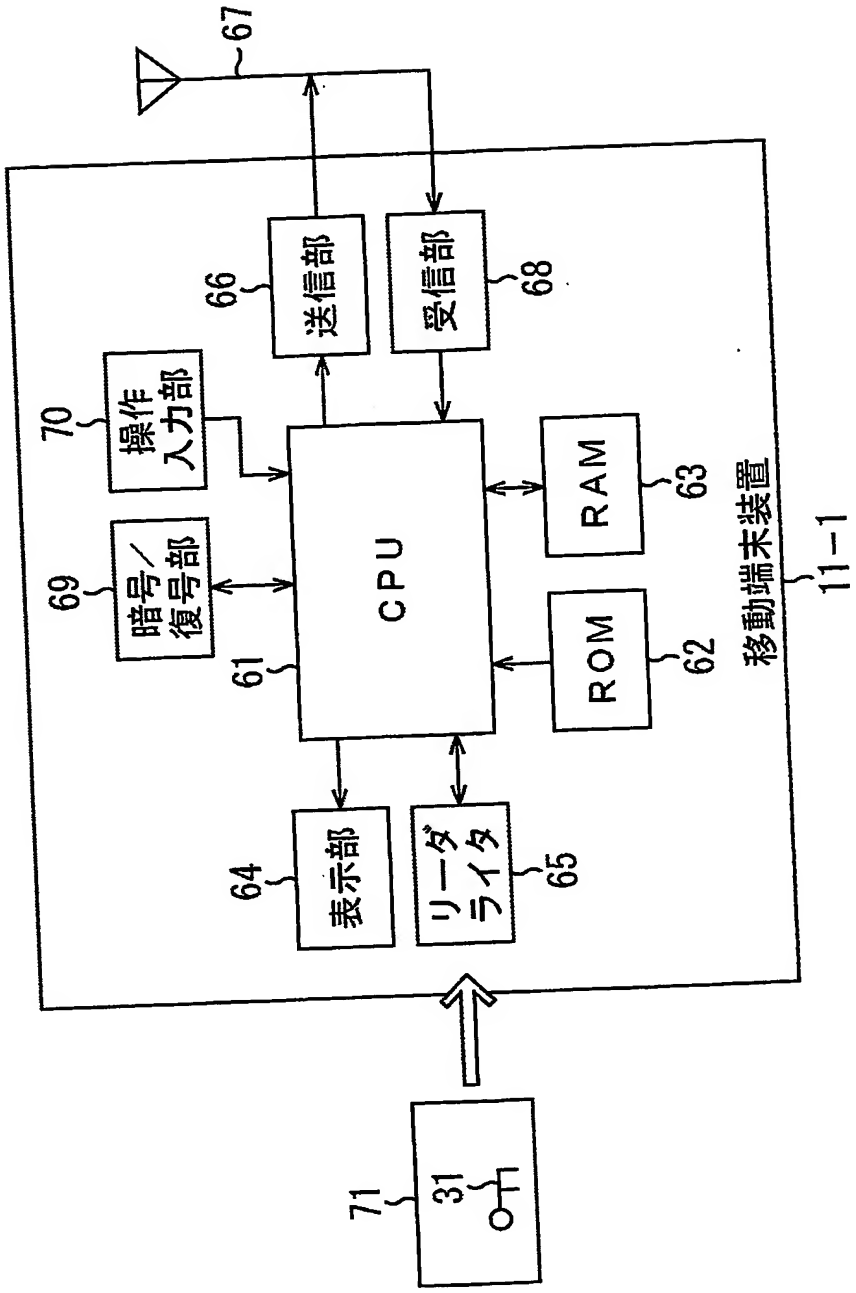
【図１】

図1


認証装置
13
41
40
39
42
バリュー発行装置
14
44
43
親機
12-2
37
38
36
インターネット
21
1
リソース機器
15-1
15-2
親機
12-1
34
リソース機器
16-1
16-2
33
35
移動端末装置
11-1
31
移動端末装置
11-2
32

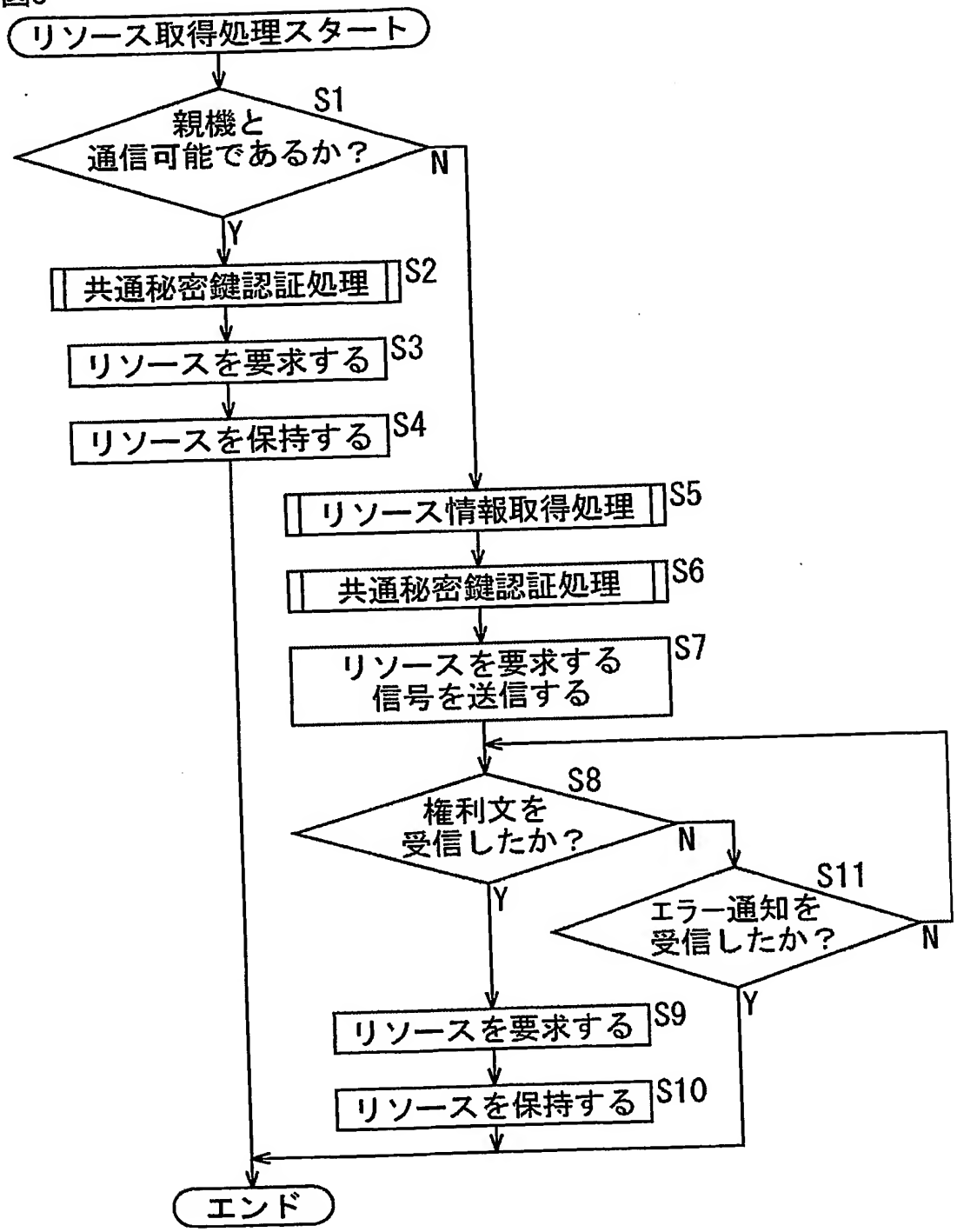
【図２】

図2


67
66
送信部
68
受信部
70
操作入力部
69
暗号／復号部
61
CPU
RAM
63
ROM
62
移動端末装置
11-1
64
表示部
リーダライタ
65
71
31

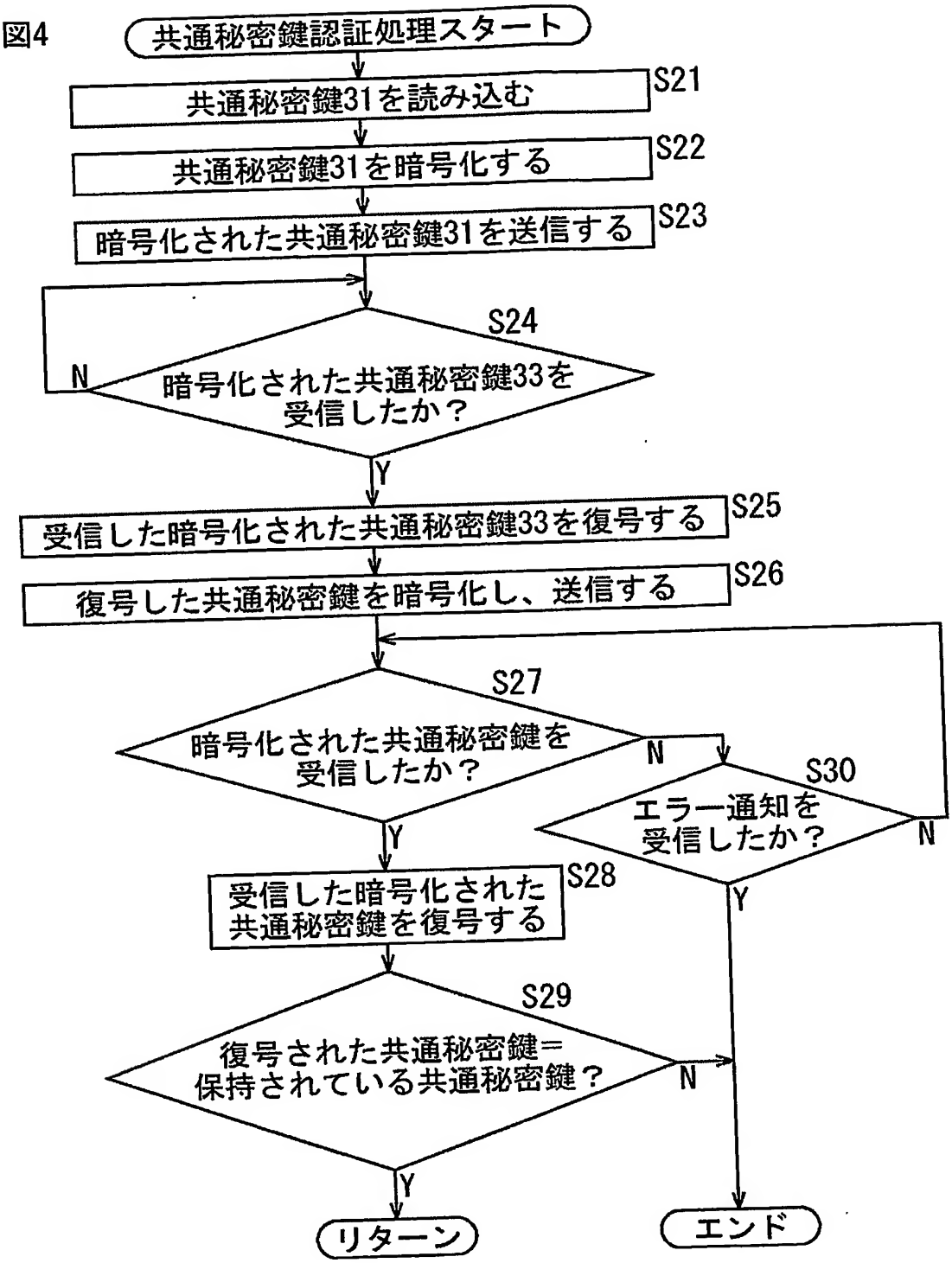
【図３】

図3


リソース取得処理スタート
S1
親機と
通信可能であるか？
N
Y
共通秘密鍵認証処理
S2
リソースを要求する
S3
リソースを保持する
S4
リソース情報取得処理
S5
共通秘密鍵認証処理
S6
リソースを要求する
信号を送信する
S7
S8
権利文を
受信したか？
N
Y
S11
エラー通知を
受信したか？
N
Y
リソースを要求する
S9
リソースを保持する
S10
エンド

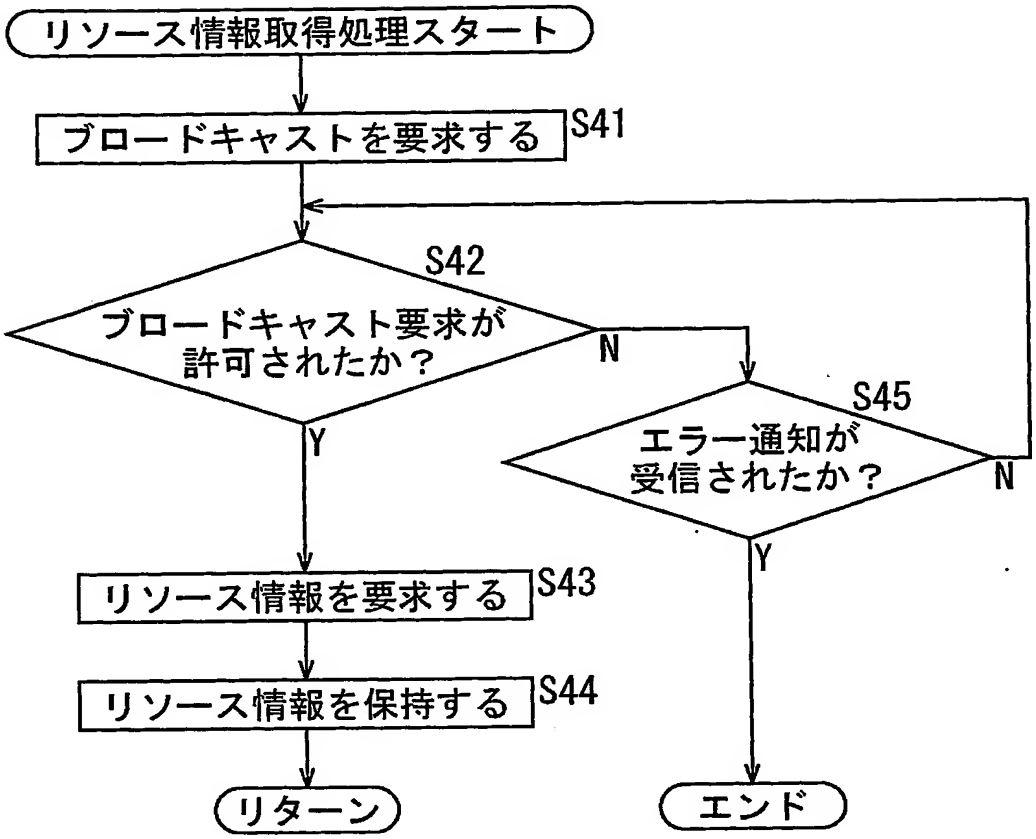
【図４】

図4


共通秘密鍵認証処理スタート
共通秘密鍵31を読み込む
S21
共通秘密鍵31を暗号化する
S22
暗号化された共通秘密鍵31を送信する
S23
S24
暗号化された共通秘密鍵33を受信したか？
N
Y
受信した暗号化された共通秘密鍵33を復号する
S25
復号した共通秘密鍵を暗号化し、送信する
S26
S27
暗号化された共通秘密鍵を受信したか？
N
Y
S30
エラー通知を受信したか？
N
Y
受信した暗号化された共通秘密鍵を復号する
S28
S29
復号された共通秘密鍵＝保持されている共通秘密鍵？
N
Y
リターン
エンド

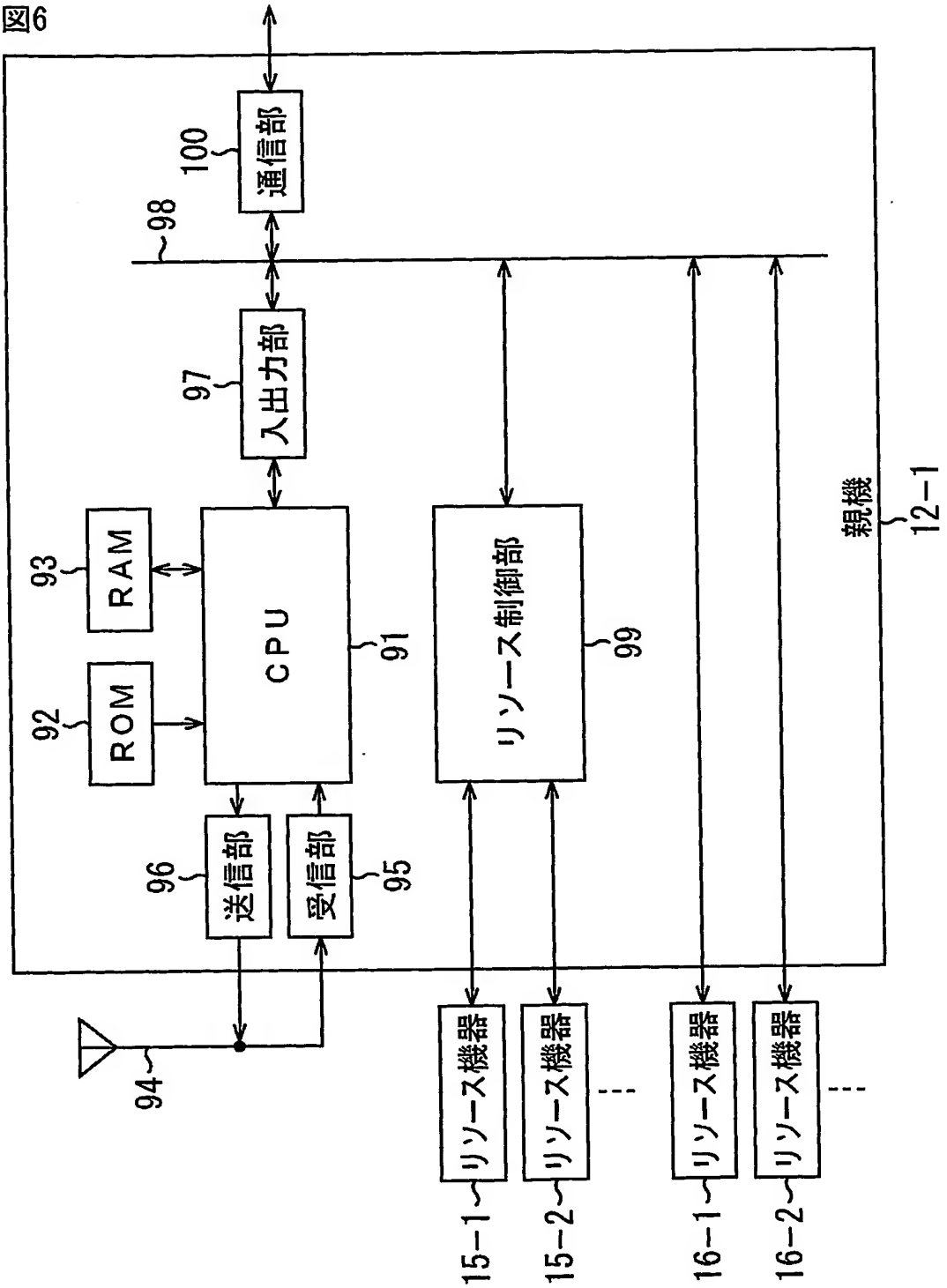
【図５】

図5


リソース情報取得処理スタート
ブロードキャストを要求する
S41
S42
ブロードキャスト要求が
許可されたか？
N
Y
S45
エラー通知が
受信されたか？
N
Y
リソース情報を要求する
S43
リソース情報を保持する
S44
リターン
エンド

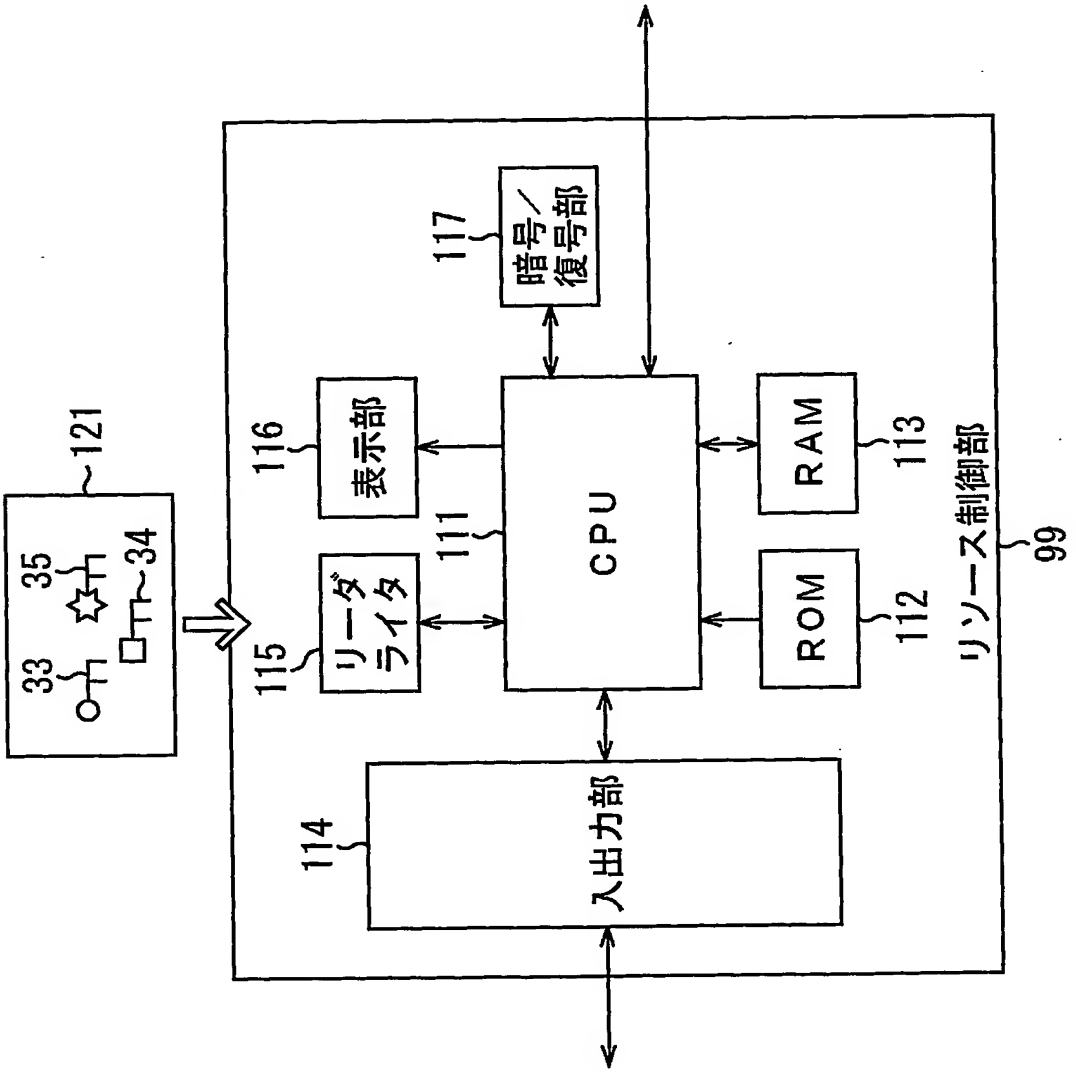
【図６】

図6


通信部
100
98
入出力部
97
RAM
93
ROM
92
CPU
91
リソース制御部
99
親機
12-1
送信部
96
受信部
95
94
リソース機器
15-1
リソース機器
15-2
リソース機器
16-1
リソース機器
16-2

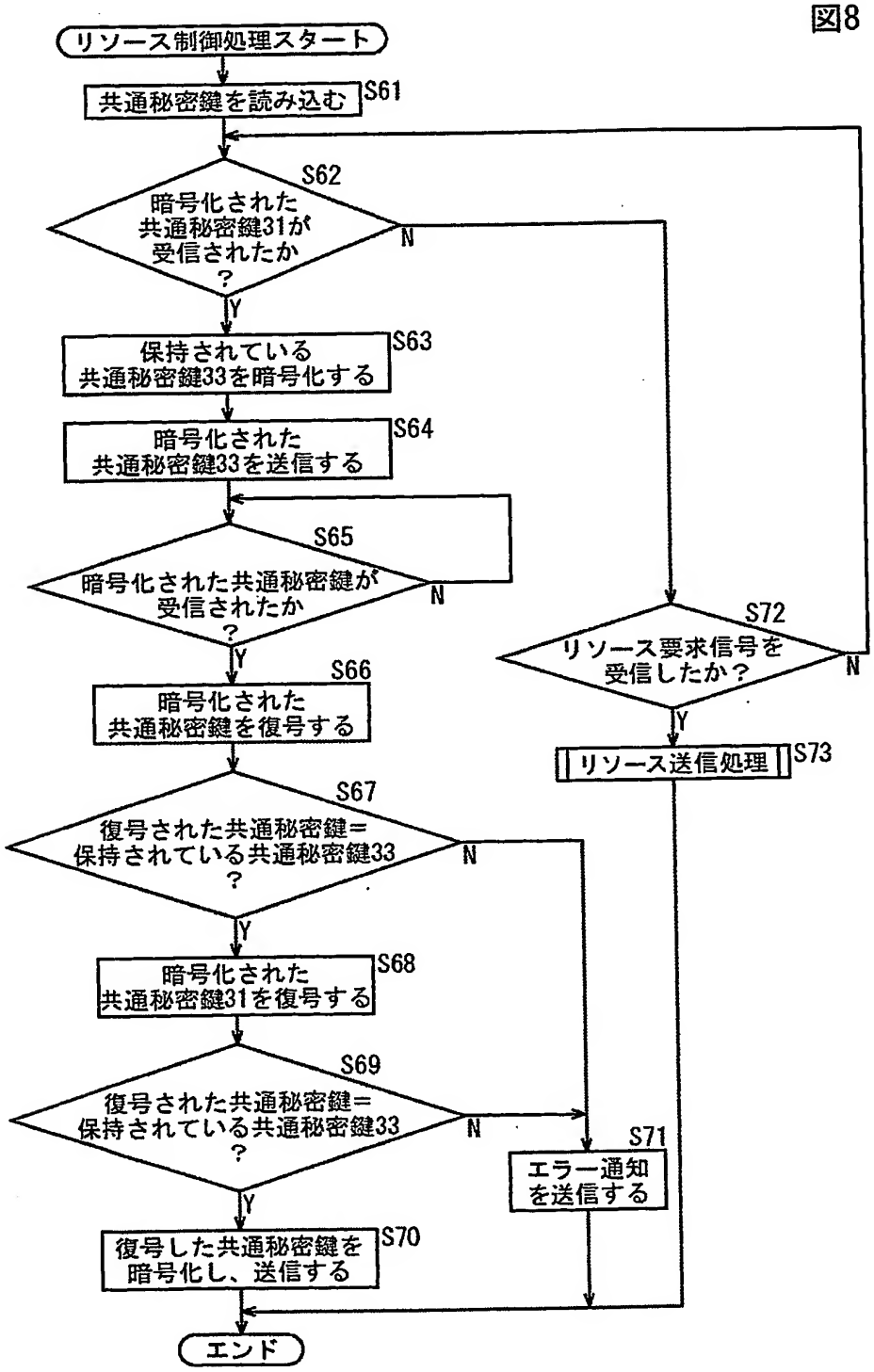
【図７】

図7


121
35
34
33
115
リーダライタ
116
表示部
111
CPU
117
暗号／復号部
RAM
113
ROM
112
114
入出力部
リソース制御部
99

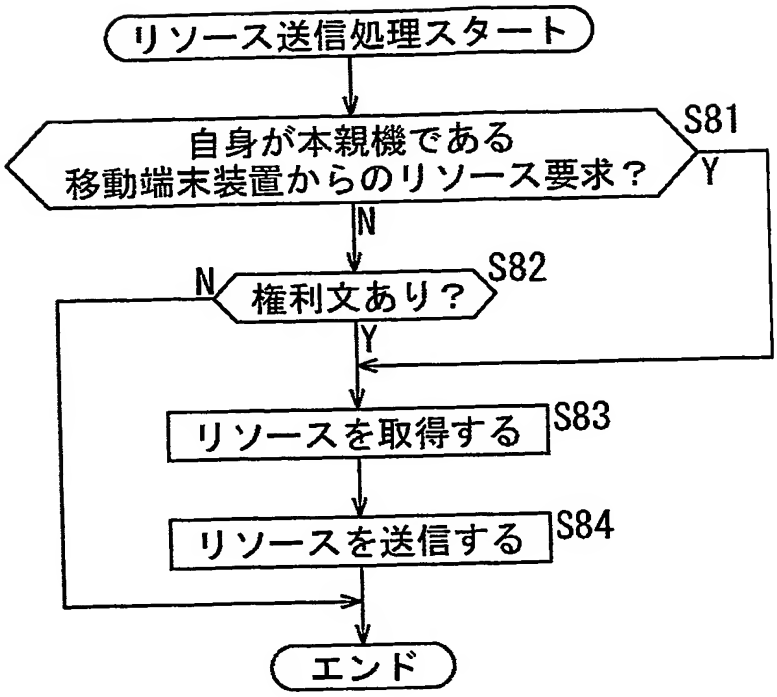
【図８】

図8


リソース制御処理スタート
共通秘密鍵を読み込む
S61
S62
暗号化された共通秘密鍵31が受信されたか？
N
Y
保持されている共通秘密鍵33を暗号化する
S63
暗号化された共通秘密鍵33を送信する
S64
S65
暗号化された共通秘密鍵が受信されたか？
N
Y
暗号化された共通秘密鍵を復号する
S66
S67
復号された共通秘密鍵＝保持されている共通秘密鍵33？
N
Y
暗号化された共通秘密鍵31を復号する
S68
S69
復号された共通秘密鍵＝保持されている共通秘密鍵33？
N
Y
復号した共通秘密鍵を暗号化し、送信する
S70
エンド
S72
リソース要求信号を受信したか？
N
Y
リソース送信処理
S73
S71
エラー通知を送信する

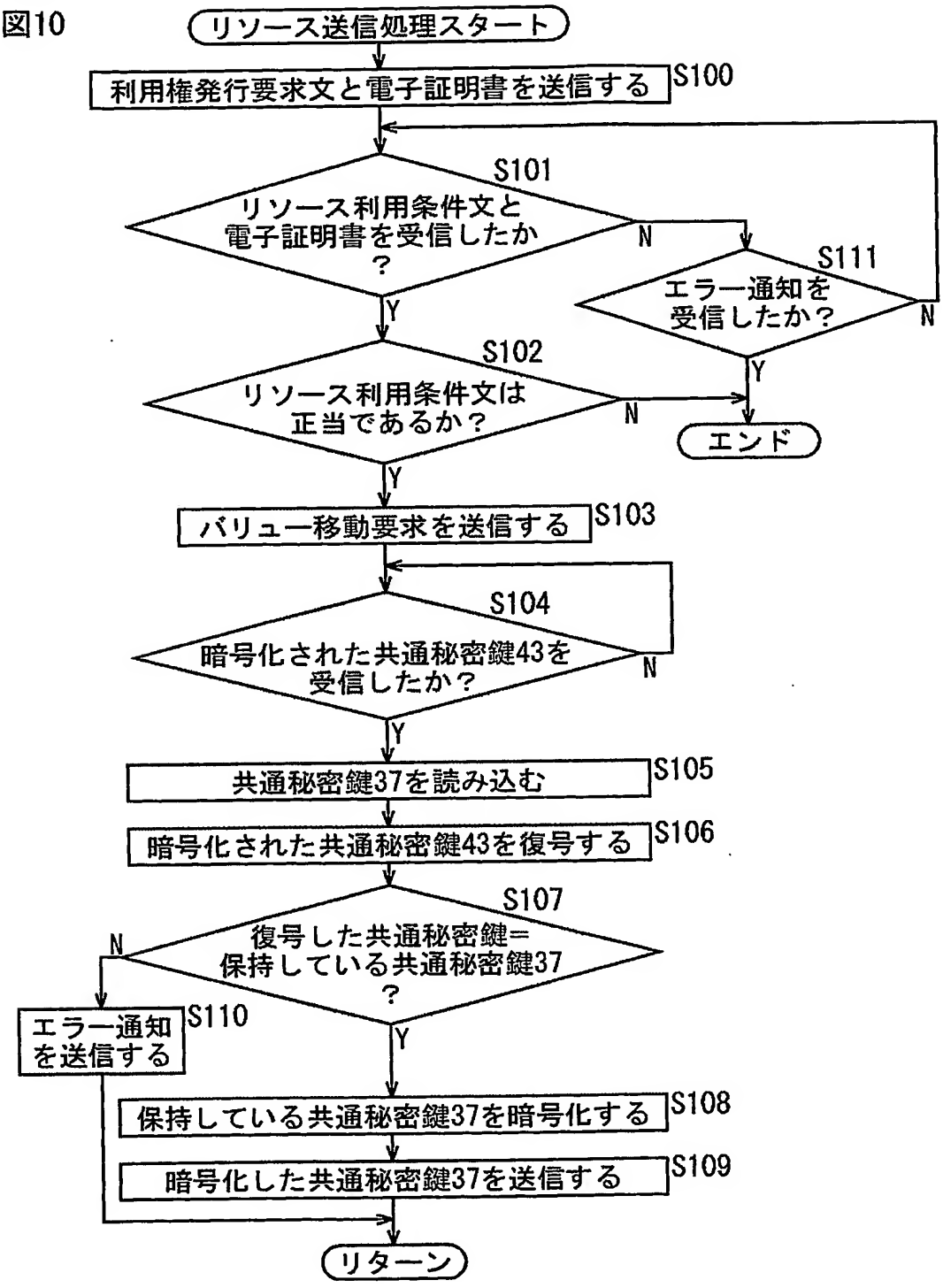
【図９】

図9


リソース送信処理スタート
自身が本親機である
移動端末装置からのリソース要求？
S81
Y
N
N
権利文あり？
S82
Y
リソースを取得する
S83
リソースを送信する
S84
エンド

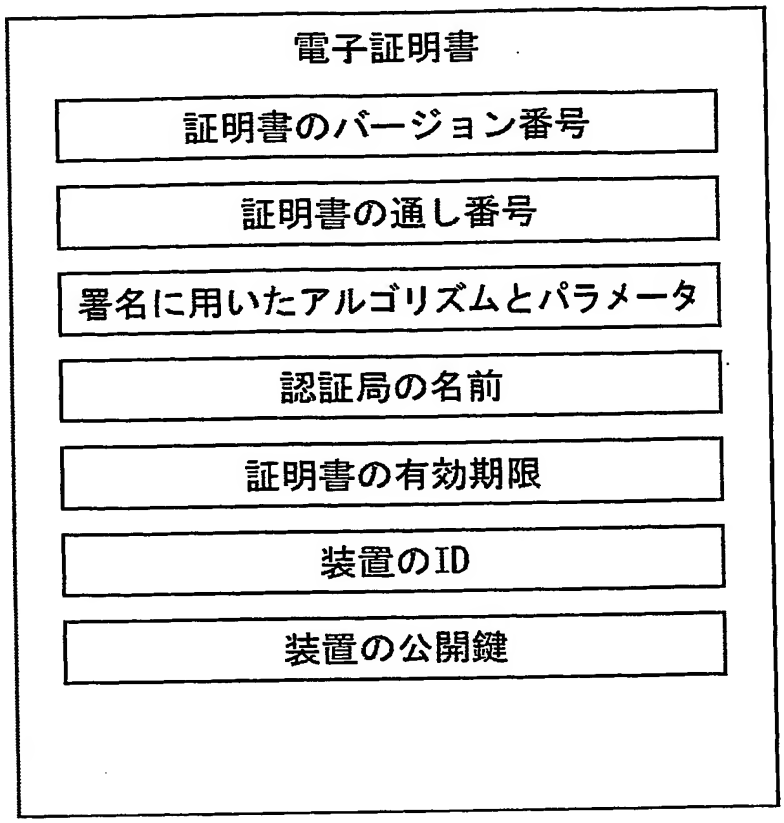
【図１０】

図10


リソース送信処理スタート
利用権発行要求文と電子証明書を送信する
S100
S101
リソース利用条件文と電子証明書を受信したか？
N
Y
S111
エラー通知を受信したか？
N
Y
S102
リソース利用条件文は正当であるか？
N
Y
エンド
バリュー移動要求を送信する
S103
S104
暗号化された共通秘密鍵43を受信したか？
N
Y
共通秘密鍵37を読み込む
S105
暗号化された共通秘密鍵43を復号する
S106
S107
復号した共通秘密鍵＝保持している共通秘密鍵37？
N
Y
エラー通知を送信する
S110
保持している共通秘密鍵37を暗号化する
S108
暗号化した共通秘密鍵37を送信する
S109
リターン

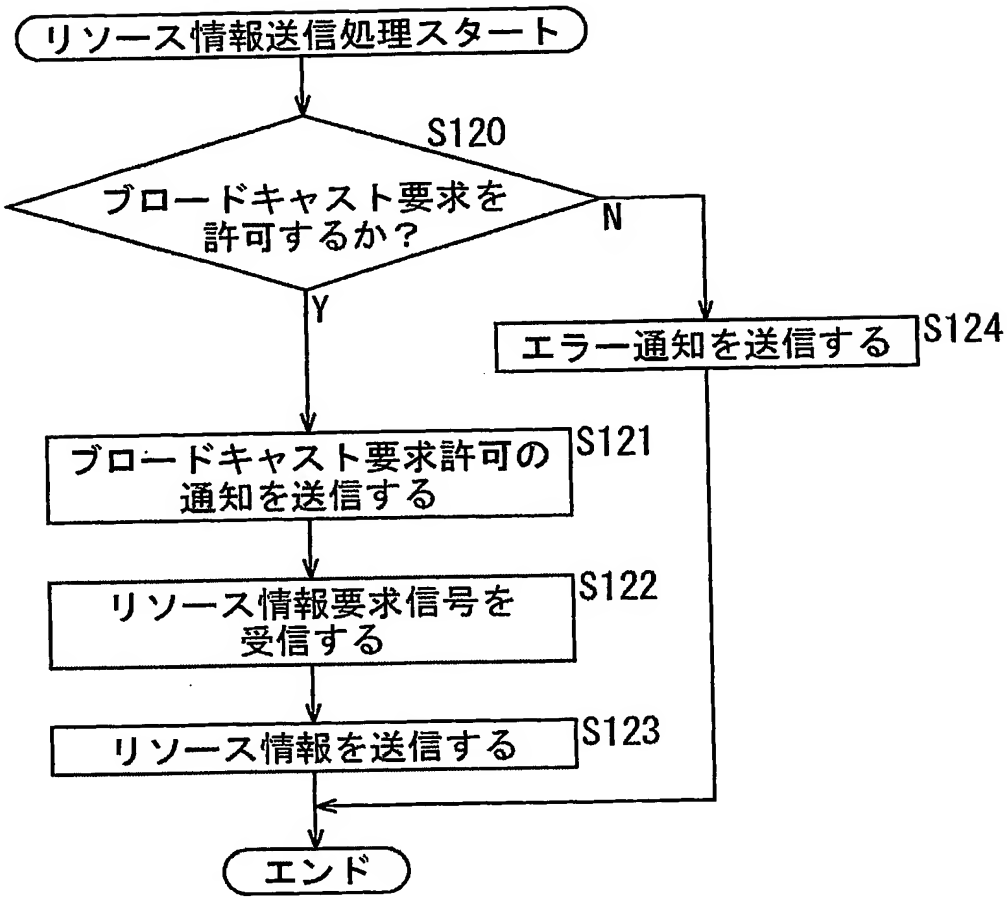
【図１１】

図11


電子証明書
証明書のバージョン番号
証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
装置のID
装置の公開鍵

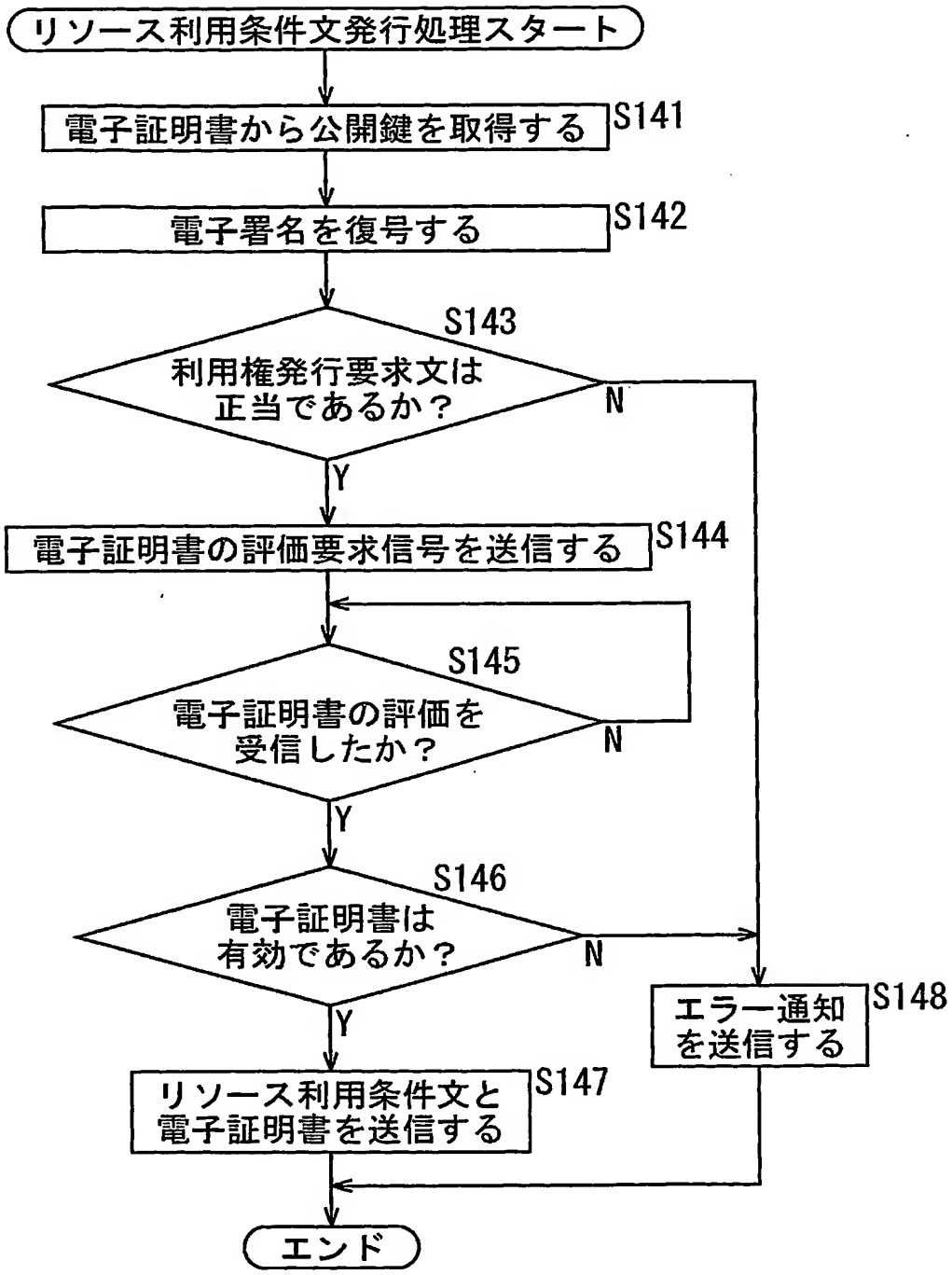
【図１２】

図12


リソース情報送信処理スタート
S120
ブロードキャスト要求を許可するか？
N
Y
エラー通知を送信する
S124
ブロードキャスト要求許可の通知を送信する
S121
リソース情報要求信号を受信する
S122
リソース情報を送信する
S123
エンド

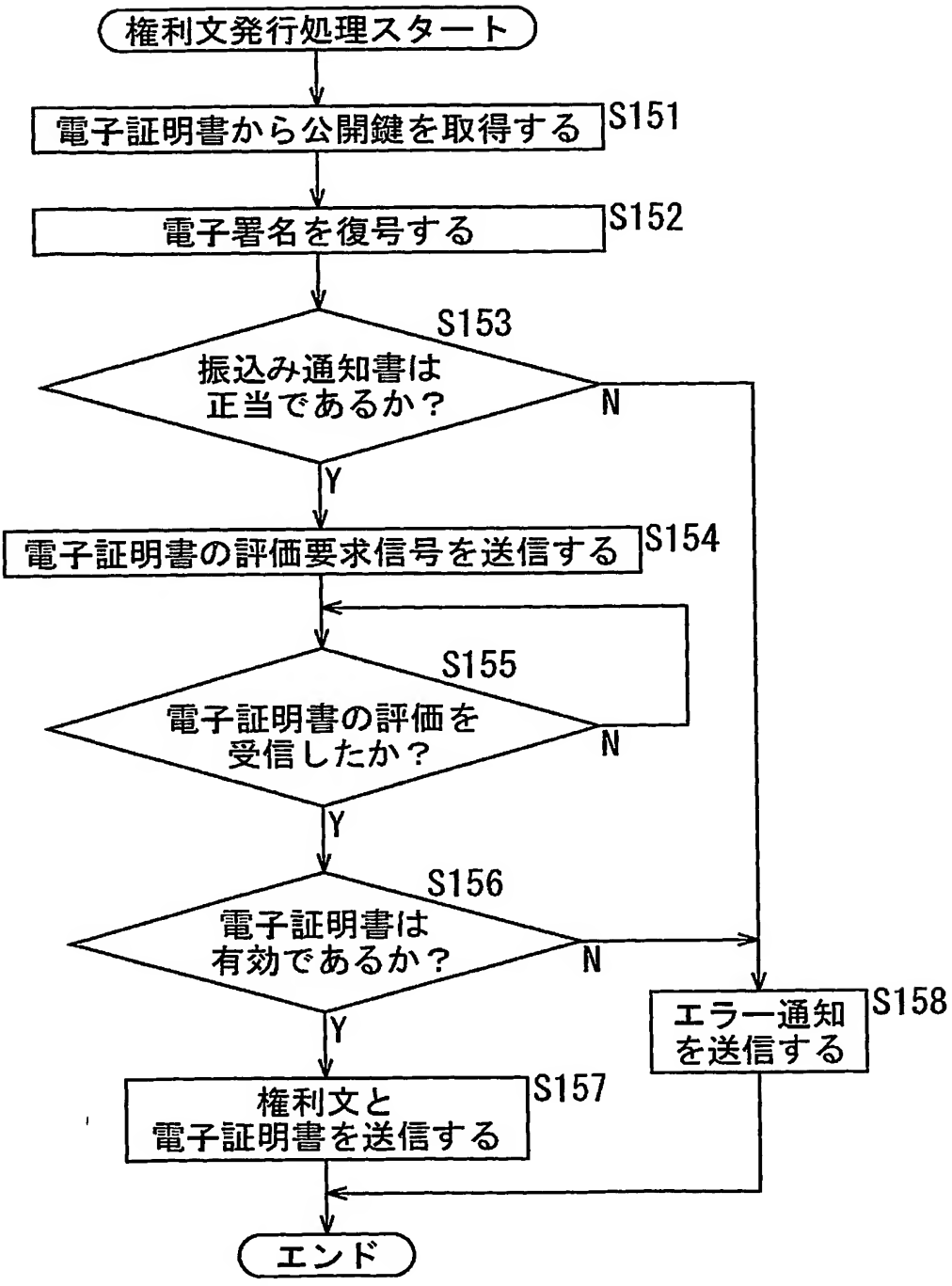
【図１３】

図13


リソース利用条件文発行処理スタート
電子証明書から公開鍵を取得する
S141
電子署名を復号する
S142
S143
利用権発行要求文は
正当であるか？
N
Y
電子証明書の評価要求信号を送信する
S144
S145
電子証明書の評価を
受信したか？
N
Y
S146
電子証明書は
有効であるか？
N
Y
エラー通知
を送信する
S148
リソース利用条件文と
電子証明書を送信する
S147
エンド

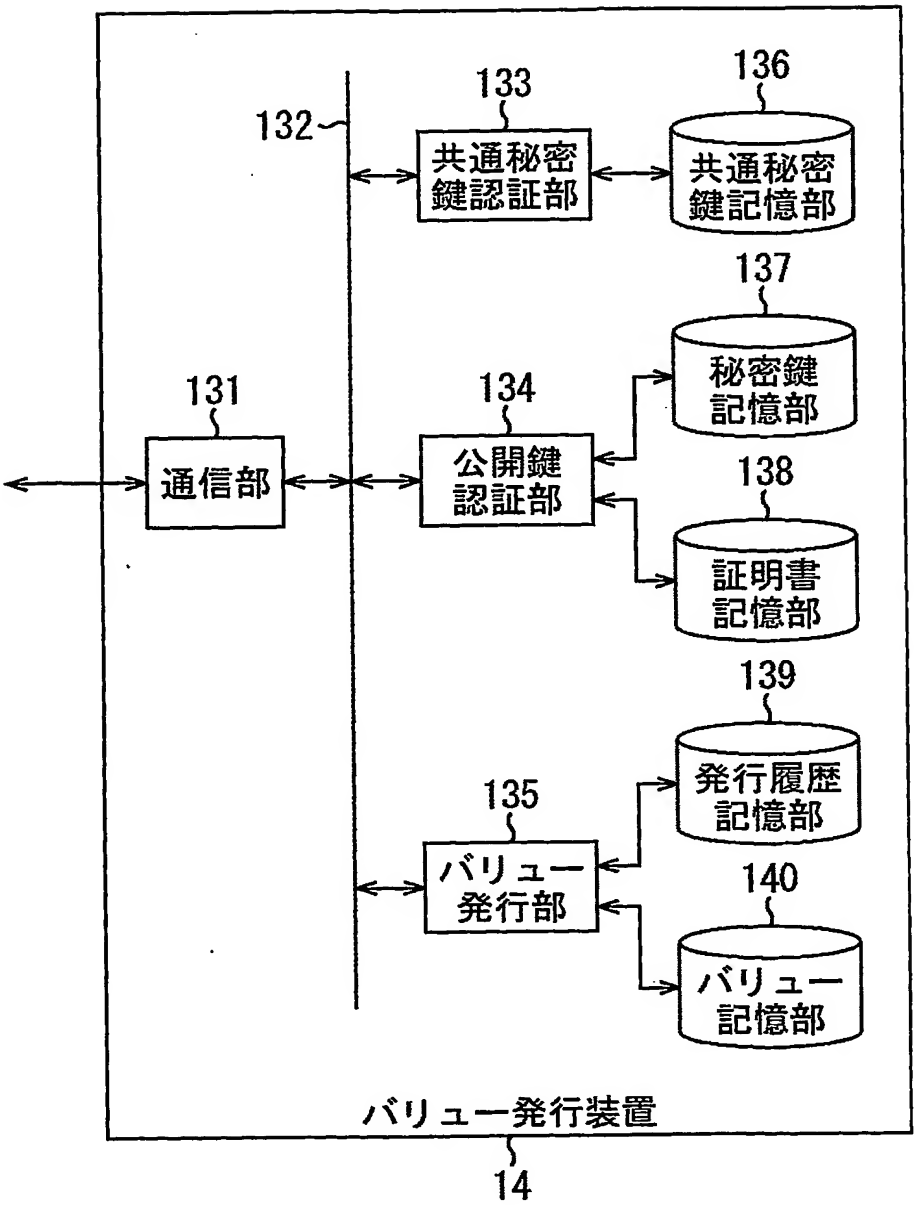
【図１４】

図14


権利文発行処理スタート
電子証明書から公開鍵を取得する
S151
電子署名を復号する
S152
S153
振込み通知書は
正当であるか？
N
Y
電子証明書の評価要求信号を送信する
S154
S155
電子証明書の評価を
受信したか？
N
Y
S156
電子証明書は
有効であるか？
N
Y
エラー通知
を送信する
S158
権利文と
電子証明書を送信する
S157
エンド

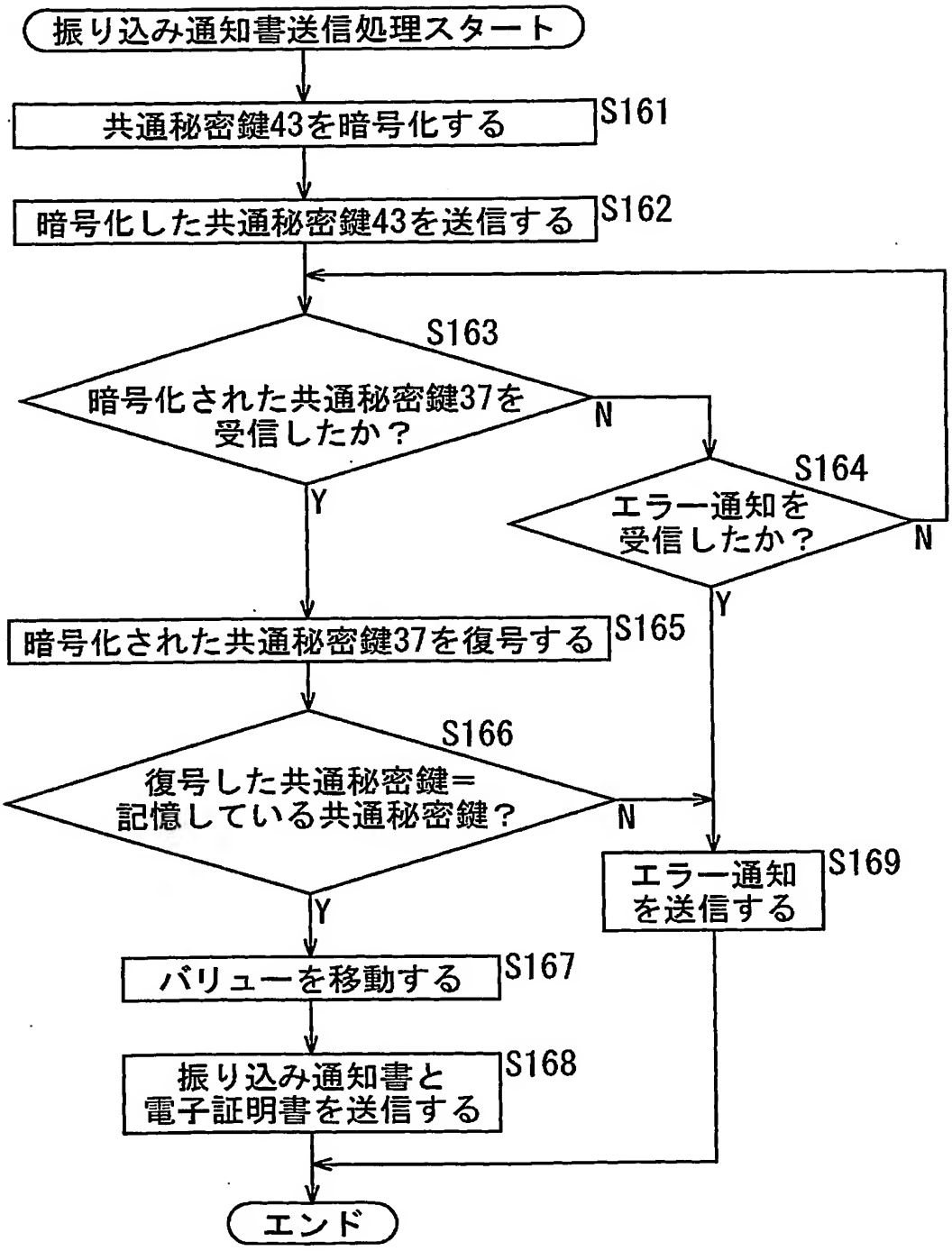
【図１５】

図15


132
133
共通秘密鍵認証部
136
共通秘密鍵記憶部
137
秘密鍵記憶部
131
通信部
134
公開鍵認証部
138
証明書記憶部
139
発行履歴記憶部
135
バリュー発行部
140
バリュー記憶部
バリュー発行装置
14

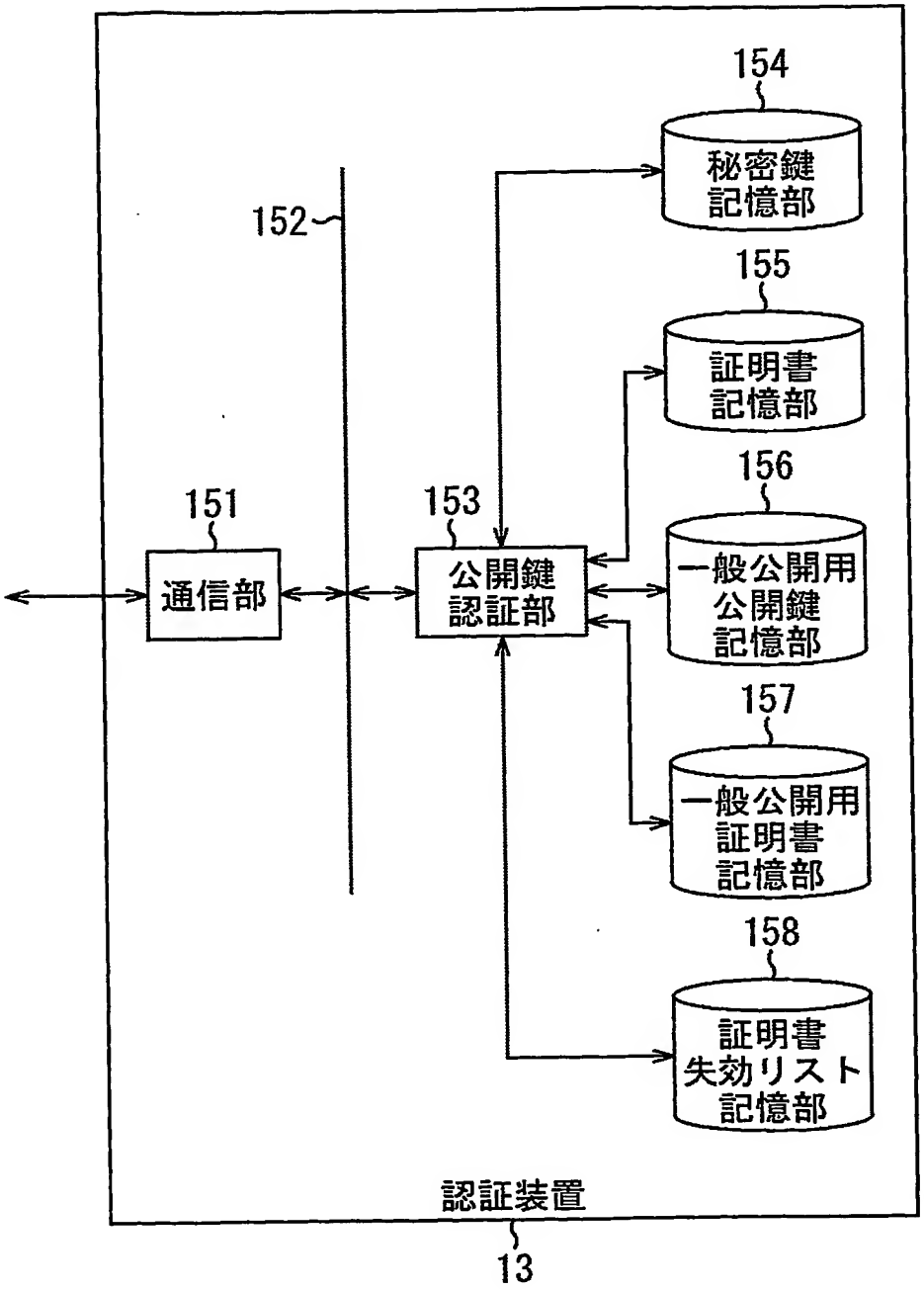
【図１６】

図16


振り込み通知書送信処理スタート
共通秘密鍵43を暗号化する
S161
暗号化した共通秘密鍵43を送信する
S162
S163
暗号化された共通秘密鍵37を受信したか？
N
Y
S164
エラー通知を受信したか？
N
Y
暗号化された共通秘密鍵37を復号する
S165
S166
復号した共通秘密鍵＝記憶している共通秘密鍵？
N
Y
エラー通知を送信する
S169
バリューを移動する
S167
振り込み通知書と電子証明書を送信する
S168
エンド

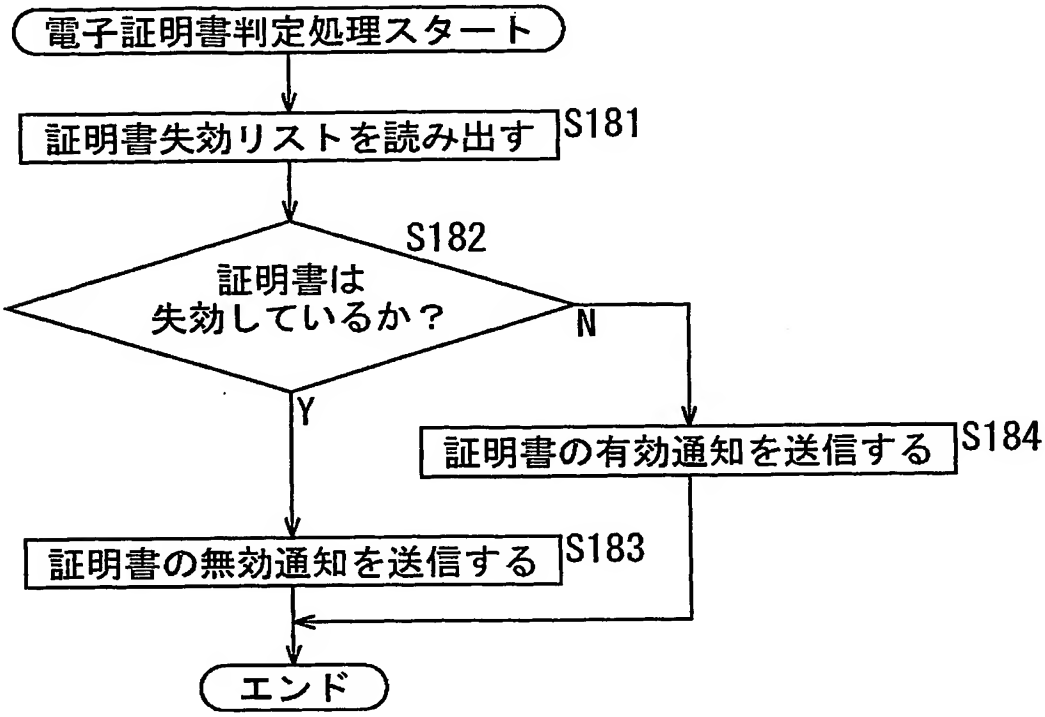
【図１７】

図17


154
秘密鍵
記憶部
152
155
証明書
記憶部
156
151
153
通信部
公開鍵
認証部
一般公開用
公開鍵
記憶部
157
一般公開用
証明書
記憶部
158
証明書
失効リスト
記憶部
認証装置
13

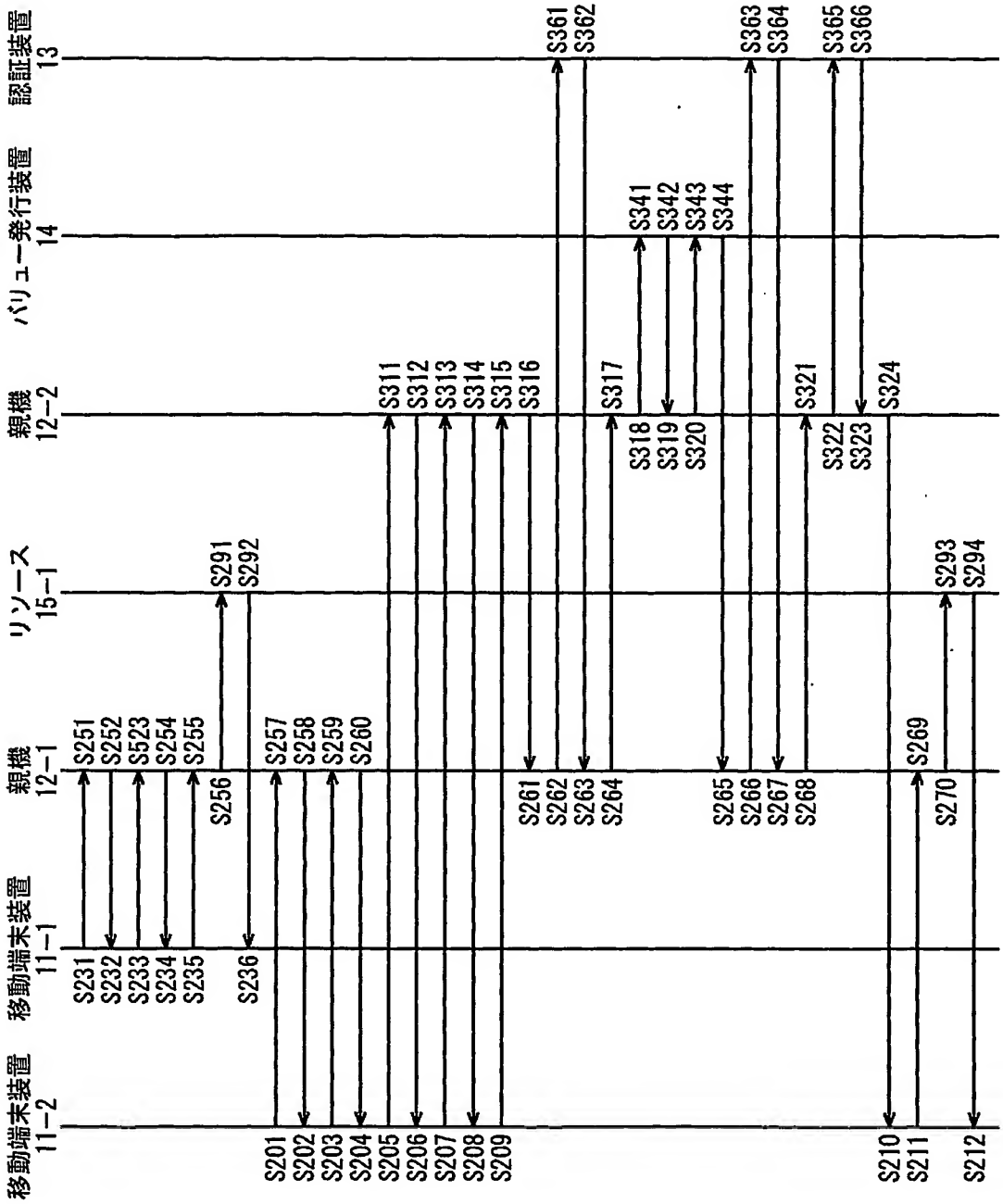
【図１８】

図18


電子証明書判定処理スタート
証明書失効リストを読み出す
S181
S182
証明書は
失効しているか？
N
Y
証明書の有効通知を送信する
S184
証明書の無効通知を送信する
S183
エンド

【図１９】

図19


移動端末装置 11-2
移動端末装置 11-1
親機 12-1
リソース 15-1
親機 12-2
バリュー発行装置 14
認証装置 13
S231
S232
S233
S234
S235
S236
S251
S252
S523
S254
S255
S256
S291
S292
S257
S258
S259
S260
S201
S202
S203
S204
S205
S206
S207
S208
S209
S311
S312
S313
S314
S315
S316
S261
S262
S263
S264
S361
S362
S317
S318
S319
S320
S341
S342
S343
S344
S265
S266
S267
S268
S363
S364
S321
S322
S323
S324
S365
S366
S269
S270
S293
S294
S210
S211
S212

【書類名】　　要約書

【要約】

【課題】　ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにする。

【解決手段】　移動端末装置１１－２は、親機１２－２にリソース機器１５のリソースを要求する。親機１２－２は、親機１２－１にリソース許可を要求し、親機１２－１は、親機１２－２に対してリソースを許可するために必要な対価を通知する。親機１２－２は、バリュー発行装置１４に対価の移動を要求する。バリュー発行装置１４は、親機１２－２の対価を親機１２－１に移動し、振込み通知書を親機１２－１に送信する。親機１２－１は、その振込み通知書を受信し、リソース利用の権利を親機１２－２を経由して移動端末装置１２－２に与える。本発明は、無線通信システムに適用することができる。

【選択図】　　図１

特願２００３－０９２６４７

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社